特 許 協 力 条 約

EP ・ US PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号　５２２２１４ＷＯ０１	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０９１２８	国際出願日 （日.月.年）　２２．１２．００	優先日 （日.月.年）　２７．１２．９９
出願人（氏名又は名称） 三菱電機株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎
ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☑ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☑ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第 9 図とする。☑ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０９１２８

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷
Ｈ０４Ｑ　７／３８　　Ｈ０４Ｌ　９／１６

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ⁷
Ｈ０４Ｂ　７／２４－７／２６　　Ｈ０４Ｑ　７／００　　Ｇ０９Ｃ　１／００－５／００
Ｈ０４Ｋ　１／００－３／００　　Ｈ０４Ｌ　９／００

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　　１９７１－２００１年
日本国登録実用新案公報　　１９９４－２００１年
日本国実用新案登録公報　　１９９６－２００１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
－

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，１０－２２９９６，Ａ（三菱電機株式会社） ２３．１月．１９９８（２３．０１．９８） ＆　ＧＢ，２３１４７４１，Ａ　＆　ＣＡ，２２０５６３７，Ａ ＆　ＤＥ，１９７２１９４９，Ａ１ ＆　ＵＳ，６０１６３５０，Ａ	1-38
Ｙ	ＪＰ，７－２４５６０６，Ａ（日本電気株式会社） １９．９月．１９９５（１９．０９．９５）， （ファミリーなし）	1-38

☑ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１２．０３．０１	21.03.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	丸山　高政	5W	９５７０
	電話番号　０３－３５８１－１１０１　内線　３５７４		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，７－３２７２５７，Ａ（株式会社日立製作所） １２．１２月．１９９５（１２．１２．９５）， （ファミリーなし）	1-38
Ｙ	ＪＰ，１０－６６１５７，Ａ （ノキア　モービル　フォーンズ　リミティド） ６．３月．１９９８（０６．０３．９８） ＆　ＧＢ，２３１３９８９，Ａ　＆　ＦＲ，２７５０２７２，Ａ１ ＆　ＦＩ，９６０２３５２，Ａ　＆　ＳＥ，９７０２１７２，Ａ ＆　ＵＳ，５９８７１３７，Ａ　＆　ＥＳ，２１４３３７１，Ａ１ ＆　ＤＥ，１９７２３６５９，Ａ１ ＆　ＷＯ９７／４７１１１，Ａ１　＆　ＡＵ，９７２３７０３，Ａ ＆　ＡＵ，９７３０３４６，Ａ	1-38
Ａ	ＪＰ，５－２２２８４，Ａ（国際電気株式会社） ２９．１月．１９９３（２９．０１．９３）， （ファミリーなし）	1-38
Ｙ	D. W. Davies and W. L. Price著，上園忠弘監訳 「ネットワーク・セキュリティ」日経マグロウヒル， （昭和６０年），pp. 77－78及び121－123	9, 18, 24-26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09128

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04Q 7/38, H04L 9/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04B 7/24-7/26, H04Q 7/00, G09C 1/00-5/00,
H04K 1/00-3/00, H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-22996, A (Mitsubishi Electric Corporation), 23 January, 1998 (23.01.98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (NEC Corporation), 19 September, 1995 (19.09.95) (Family: none)	1-38
Y	JP, 7-327257, A (Hitachi, Ltd.), 12 December, 1995 (12.12.95) (Family: none)	1-38
Y	JP, 10-66157, A (Nokia Mobile Phones Ltd.), 06 March, 1998 (06.03.98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111,A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (Kokusai Electric Co., Ltd.), 29 January, 1993 (29.01.93) (Family: none)	1-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March, 2001 (12.03.01)	21 March, 2001 (21.03.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	D. W. Davies and W. L. Price; Translation supervised by Tadahiro Uezono "Network Security", Nikkei McGraw Hill (1985), pp. 77-78, pp.121-123	9,18,24-26

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年7月5日 (05.07.2001)

PCT

(10) 国際公開番号
WO 01/49058 A1

(51) 国際特許分類[7]: H04Q 7/38, H04L 9/16

(21) 国際出願番号: PCT/JP00/09128

(22) 国際出願日: 2000年12月22日 (22.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/370657
1999年12月27日 (27.12.1999) JP

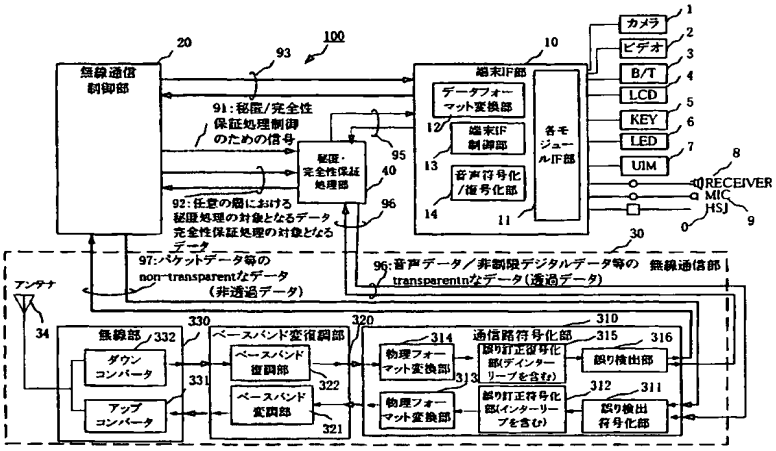
(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 宇賀晋介 (UGA,

[続葉有]

(54) Title: RADIO COMMUNICATION DEVICE AND RADIO COMMUNICATION METHOD

(54) 発明の名称: 無線通信装置及び無線通信方法



20...RADIO COMMUNICATION CONTROL UNIT
91...SIGNAL FOR CONTROL OF SECRETING/COMPLETENESS-SECURING
40...SECRETING/COMPLETENESS-SECURING UNIT
92...DATA TO BE SECRETED IN ANY LAYER AND DATA THE COMPLETENESS OF WHICH IS TO BE SECURED
10...TERMINAL IF UNIT
12...DATA FORMAT CONVERTING SECTION
13...TERMINAL IF CONTROL SECTION
14...AUDIO ENCODING/DECODING SECTION
11...MODULE IP SECTIONS
1...CAMERA
2...VIDEO
97...NON-TRANSPARENT DATA SUCH AS PACKET DATA
96...TRANSPARENT DATA SUCH AS AUDIO DATA/NON-LIMITED DATA
30...RADIO COMMUNICATION UNIT
34...ANTENNA
330...RADIO SECTION
332...DOWN CONVERTER
331...UP CONVERTER
320...BASEBAND MODULATING/DEMODULATING SECTION
322...BASEBAND DEMODULATING PART
321...BASEBAND MODULATING PART
310...COMMUNICATION LINE ENCODING SECTION
314...PHYSICAL FORMAT CONVERTING PART
313...PHYSICAL FORMAT CONVERTING PART
315...ERROR CORRECTION DECODING PART (INCLUDING DEINTERLEAVING)
312...ERROR CORRECTION ENCODING PART (INCLUDING INTERLEAVING)
316...ERROR DETECTING SECTION
311...ERROR DETECTING/CORRECTING PART

(57) Abstract: A radio terminal (MS) (100) capable of secreting and securing completeness in layer 2 or higher-order layers and comprising a terminal IF unit (10), a radio communication control unit (20), a radio communication unit (30), and a secreting/completion-securing unit (40) connected to the terminal IF unit (10), the terminal IF unit (20), and the radio communication unit (30). The secreting/completeness-securing unit (40) only secrets transparent data such as audio data with respect to the terminal IF unit (10) and the radio communication unit (30), secrets non-transparent data and/or secures the completeness of the nontransparent data with respect to the radio communication control unit (20), and selectively secrets data on layer 2 and the higher-order layers outputted from the radio communication unit (30) or secures the completeness of the data according to the type of data.

[続葉有]

WO 01/49058 A1

Shinsuke) [JP/JP]. 松山浩司 (MATSUYAMA, Hiroshi) [JP/JP]. 近澤　武 (CHIKAZAWA, Takeshi) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).

(81) 指定国 (国内): AU, CA, CN, JP, KR, MX, NO, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

レイヤ２以上の上位レイヤにおいて秘匿処理及び完全性保証処理が行える無線端末（ＭＳ）１００を提供したい。端末ＩＦ部１０と無線通信制御部２０と無線通信部３０との間に秘匿・完全性保証処理部４０を設ける。秘匿・完全性保証処理部４０は、端末ＩＦ部１０と無線通信部３０との間で音声データ等の透過データに対して秘匿処理のみを行う。秘匿・完全性保証処理部４０は、無線通信制御部２０との間で非透過データに対して秘匿処理又は／及び完全性保証処理を行う。秘匿・完全性保証処理部４０は、無線通信部３０から出力されたレイヤ２以上の上位階層のデータに対してデータの種別に応じて選択的に秘匿処理、完全性保証処理を行う。

明　細　書

無線通信装置及び無線通信方法

技術分野

この発明は、携帯電話機等の無線通信装置及び無線通信方法に関するものである。特に、データの秘匿処理と完全性保証処理を行う携帯電話機に関するものである。

背景技術

図２４は、従来の携帯電話機５００を示す図である。

従来の携帯電話機５００には、端末ＩＦ（インタフェース）部５１０と無線通信制御部５２０と無線通信部５３０が備えられている。端末ＩＦ部５１０は、携帯電話機５００のユーザとのインタフェースを行う部分である。無線通信制御部５２０は、携帯電話機５００全体の通信制御とプロトコルに基づくデータの変換とデータ処理とを行う部分である。無線通信部５３０は、データを変調復調し、無線通信可能とする部分である。無線通信部５３０は、ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍｓ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）で定義されている７階層のレイヤの内、最下層である物理レイヤ（レイヤ１）をサポートしている部分である。無線通信部５３０には、秘匿処理部５４０が設けられている。秘匿処理部５４０は、無線通信部５３０で取り扱われる物理レイヤのデータに対して暗号化処理、或いは、復号化処理を行う部分である。秘匿処理部５４０を設けることによりアンテナ５４１で送受信されるデータを盗聴しても暗号化されているので、解読されない限りにおいて盗聴者が有意な情報を得ることはできないこととなる。

従来の携帯電話機５００は、秘匿処理部５４０を無線通信部５３０の内部に有している。このため、秘匿処理部５４０が秘匿対象とするデータは、物理レイヤ（レイヤ１）のデータである。物理レイヤでは、そのデータがユーザデータであるか制御データであるかは特定できない。携帯電話機により送受信されるデータの中には、各種ユーザデータ及びシグナリングデータなどいろいろな種類があり、そのデータの種類に応じて秘匿処理を行ったり、或いは、そのデータの重要性に応じてデータの完全性を保証したりする必要がある。従来の構成のように、秘匿処理部５４０がレイヤ１に設けられていたのでは、レイヤ１においてはデータの種別が区別できないため、データの種別に応じて秘匿処理や完全性の保証をするということができなかった。

この発明の好適な実施の形態では、データの種類に応じて秘匿処理や完全性保証処理が選択的に行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、ＯＳＩの７つの階層の内、レイヤ２（データリンク層）以上の上位レイヤにおいて秘匿処理と完全性保証処理が行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、秘匿処理と完全性保証処理との両方又は一方をデータの種類に応じて選択的に行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、無線通信装置が複数のチャネルを有している場合においてもチャネル毎に秘匿処理と完全性保証処理とが行える無線通信装置及び無線通信方法を得ることを目的とする。

また、この発明の好適な実施の形態では、あるレイヤ、或いは、サブレイヤを透過する透過データと、そのレイヤ、或いは、サブレイヤを透

過しない非透過データとを区別して、秘匿処理と完全性保証処理とを選択的に行う無線通信装置及び無線通信方法を得ることを目的とする。

発明の開示

この発明に係る無線通信装置は、データを入力する端末インタフェース部と、

端末インタフェース部が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

無線通信制御部から出力されたデータを入力して変調し送信する無線通信部と

を備えたことを特徴とする。

上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて端末インタフェース部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを無線通信部に出力することを特徴とする。

上記端末インタフェース部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを端末インタフェース部から入

力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを端末インタフェース部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする。

上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

上記秘匿・完全性保証処理部は、
入力したデータを暗号化する暗号化部を有する秘匿処理部と、
入力したデータに対して完全性認証子を付加する完全性認証子付加部を有する完全性保証処理部と
を備えたことを特徴とする。

上記秘匿処理部は、複数の暗号化部を有することを特徴とする。

上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする。

上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する１つのモジュールであり、その１つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行するこ

とを特徴とする。

この発明に係る無線通信装置は、データを受信して復調する無線通信部と、

無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と

を備えたことを特徴とする。

上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを端末インタフェース部に出力することを特徴とする。

上記無線通信部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理

させることを特徴とする。

上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする。

上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする。

上記秘匿・完全性保証処理部は、
入力したデータを復号化する復号化部を有する秘匿処理部と、
入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部と
を備えたことを特徴とする。

上記秘匿処理部は、複数の復号化部を有することを特徴とする。

上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする。

上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する１つのモジュールであり、その１つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする。

この発明に係る無線通信装置は、データを無線通信する無線通信装置において、

データを入出力する端末インタフェース部と、

プロトコルに基づいてデータの処理をする無線通信制御部と、

データを無線通信する無線通信部と、

端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、無線通信制御部との間でデータに対して少なくともデータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース部から無線通信部へのデータを暗号化するとともに無線通信部から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部と

を備えたことを特徴とする。

上記秘匿・完全性保証処理部は、

入力したデータに対して秘匿処理を行う秘匿処理部と、

入力したデータに対して完全性保証処理を行う完全性保証処理部と

を個別に備えたことを特徴とする。

上記秘匿処理部は、

端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、

無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個別に有することを特徴とする。

上記完全性保証処理部は、

入力したデータに対して完全性保証処理を行う完全性認証子を付加す

る完全性認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部と

を個別に有することを特徴とする。

上記通信装置は、携帯型移動電話機であることを特徴とする。

上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする。

上記無線通信装置は、携帯電話機であることを特徴とする。

上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする。

上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする。

この発明に係る無線通信方法は、データを入力する端末インタフェース工程と、

端末インタフェース工程が入力したデータを入力し、データを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全

性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

無線通信制御工程から出力されたデータを入力して変調し送信する無線通信工程と

を備えたことを特徴とする。

この発明に係る無線通信方法は、データを受信して復調する無線通信工程と、

無線通信工程により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

無線通信制御工程により処理されたデータを入力して出力する端末インタフェース工程と

を備えたことを特徴とする。

この発明に係る無線通信方法は、データを無線通信する無線通信方法において、

データを入出力する端末インタフェース工程と、

プロトコルに基づいてデータの処理をする無線通信制御工程と、

データを無線通信する無線通信工程と、

端末インタフェース工程と無線通信制御工程と無線通信工程との三者間に設けられ、無線通信制御工程との間でデータに対して少なくともデ

ータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース工程から無線通信工程へのデータを暗号化するとともに無線通信工程から端末インタフェース工程へのデータを復号する秘匿・完全性保証処理工程と

を備えたことを特徴とする。

図面の簡単な説明

図１は、移動体通信システムの構成図。

図２は、無線制御局（ＲＮＣ）１２０の構成図。

図３は、実施の形態１の無線端末（ＭＳ）１００の構成図。

図４は、実施の形態１の秘匿・完全性保証処理部４０の構成図。

図５は、実施の形態１の秘匿・完全性保証処理部４０の構成図。

図６は、実施の形態１の秘匿・完全性保証処理部４０の構成図。

図７は、実施の形態１の秘匿・完全性保証処理部４０の構成図。

図８は、実施の形態１の秘匿・完全性保証処理部４０の構成図。

図９は、実施の形態２の無線端末（ＭＳ）１００の構成図。

図１０は、実施の形態２の秘匿・完全性保証処理部４０の構成図。

図１１は、実施の形態２の秘匿・完全性保証処理部４０の構成図。

図１２は、暗号化方式及び復号化方式の一例を示す図。

図１３は、実施の形態２の秘匿・完全性保証処理部４０の構成図。

図１４は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｓｅｃｔｉｏｎ　６．３．に示された図。

図１５は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｆｉｇｕｒｅ　１６ｂ．に示された図。

図１６は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｆｉｇｕｒｅ　１６．に示された図。

図１７は、暗号化／復号化部４２１の中で用いられる暗号化モジュール５１（又は復号化モジュール７１）の構成図。

図１８は、秘匿・完全性保証処理部４０の実装形式を示す図。

図１９は、秘匿・完全性保証処理部４０をソフトウェアで実現する場合を示す図。

図２０は、無線通信制御部２０で動作するアプリケーションプログラム４６が暗号化プログラム４７を呼び出すメカニズムを示す図。

図２１は、ＲＬＣ非透過モードのときのデータ９２，９３の具体例を示す図。

図２２は、透過データ９５，９６の一例として音声データの具体例を示す図。

図２３は、透過データ９５，９６の一例として非制限デジタルデータの具体例を示す図。

図２４は、従来の携帯電話機５００を示す図。

発明を実施するための最良の形態

実施の形態１．

図１は、この実施の形態の移動体通信システムの全体構成図である。

無線端末（ＭＳ）１００は、この発明の無線通信装置の一例である。無線端末（ＭＳ）１００は、例えば、携帯電話機である。無線端末（ＭＳ）１００は、無線で無線基地局（ＢＴＳ）１１０と接続される。無線基地局（ＢＴＳ）１１０は、無線制御局（ＲＮＣ）１２０と接続される。無線制御局（ＲＮＣ）１２０は、他の無線制御局（ＲＮＣ）１２０と

接続される。また、無線制御局（ＲＮＣ）１２０は、コアネットワーク（ＣＮ）１３０に接続され、コアネットワーク（ＣＮ）１３０を介して他の無線制御局（ＲＮＣ）１２０と接続される。無線基地局（ＢＴＳ）１１０と無線制御局（ＲＮＣ）１２０とのいずれか又は両方は、無線局とも呼ばれる。

図２は、図１と同じ移動体通信システムの構成図である。特に、無線制御局（ＲＮＣ）１２０の内部の構成を示している。

ＢＴＳ　ＩＦ部１２１は、無線基地局（ＢＴＳ）１１０を接続する。ハンドオーバ制御部１２２は、無線基地局（ＢＴＳ）１１０間を無線端末（ＭＳ）１００が移動する場合のハンドオーバを制御する。

対ＭＳ信号制御部１２３は、無線端末（ＭＳ）１００との間での無線通信制御及びデータの秘匿処理／完全性保証処理を行う。以下に述べる無線端末（ＭＳ）１００の秘匿処理及び完全性保証処理は、対ＭＳ信号制御部１２３の秘匿処理及び完全性保証処理に対応して行われるものである。即ち、無線端末（ＭＳ）１００において暗号化されたデータは、対ＭＳ信号制御部１２３において復号化される。逆に、対ＭＳ信号制御部１２３で暗号化されたデータは、無線端末（ＭＳ）１００において復号化される。また、無線端末（ＭＳ）１００においてデータの完全性を保証するために付加された認証子は、対ＭＳ信号制御部１２３において検証される。逆に、対ＭＳ信号制御部１２３においてデータの完全性を保証するために付加された認証子は、無線端末（ＭＳ）１００において検証される。この無線端末（ＭＳ）１００と対ＭＳ信号制御部１２３におけるデータの秘匿処理及びデータの完全性保証処理は、ＯＳＩの７つの階層の内の２番目のレイヤ、即ち、レイヤ２（データリンク層）で行われる。ＣＮ　ＩＦ部１２４は、コアネットワーク（ＣＮ）１３０とのインタフェースをとる。

ＲＮＣ　ＩＦ部１２５は、他の無線制御局（ＲＮＣ）１２０とのインタフェースをとる。対ＣＮ信号制御部１２６は、コアネットワーク（ＣＮ）１３０との間での制御を行う。対ＲＮＣ信号制御部１２７は、他の無線制御局（ＲＮＣ）１２０との間で制御を行う。制御部１２８は、無線制御局（ＲＮＣ）１２０全体を制御する。スイッチ１２９は、制御部１２８の制御に基づいて、無線基地局（ＢＴＳ）１１０と無線制御局（ＲＮＣ）１２０とコアネットワーク（ＣＮ）１３０との間で制御信号並びにパケットデータをスイッチングする。即ち、スイッチ１２９は、パケットデータだけでなく、音声等を含む全てのデータをスイッチするとともに、制御信号もスイッチする。

図３は、無線端末（ＭＳ）１００の構成図である。

無線端末（ＭＳ）１００は、端末ＩＦ部１０と無線通信制御部２０と無線通信部３０と秘匿・完全性保証処理部４０を有している。端末ＩＦ部１０は、カメラ１とビデオ２とＢ／Ｔ（Ｂｌｕｅ　Ｔｏｏｔｈ）３とＬＣＤ４とＫＥＹ５とＬＥＤ６とＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）７とＲＥＣＥＩＶＥＲ８とＭＩＣ９とＨＳＪ（Ｈｅａｄ　Ｓｅｔ　Ｊａｃｋ）０とを接続している。これらのカメラ１からＨＳＪ０は、ユーザ（人間）もしくは接続の対象となる機器とのインターフェースのための処理を行い、ユーザ（人間）もしくは接続の対象となる機器が認識できる情報を入力又は出力するものである。

端末ＩＦ部１０は、内部に各モジュールＩＦ部１１とデータフォーマット変換部１２と端末ＩＦ制御部１３と音声符号化／復号化部１４を有している。各モジュールＩＦ部１１は、カメラ１からＨＳＪ０との各インタフェースをとる。データフォーマット変換部１２は、カメラ１からＨＳＪ０で取り扱う各データフォーマットと無線端末（ＭＳ）１００内

部で取り扱う各データフォーマットとの間での変換を行う。端末ＩＦ制御部１３は、端末ＩＦ部１０の動作を制御する。音声符号化／復号化部１４は、ＭＩＣ９から入力された音声電気信号を音声符号化する。また、音声符号化／復号化部１４は、音声符号化された信号を復号してＲＥＣＥＩＶＥＲ８に対して音声電気信号を出力する。

無線通信制御部２０は、無線端末（ＭＳ）１００の全体制御を行う。無線通信制御部２０には、ＣＰＵ、ＲＯＭ、ＲＡＭ、ファームウェア等からなるハードウェア回路、或いは、ソフトウェアモジュールが備えられている。無線通信制御部２０は、端末ＩＦ部１０と無線通信部３０との間でデータを処理するものであり、規格或いはプロトコルにより定められた規則に基づいてデータの変換処理を行う。特に、レイヤ２以上の処理を行う。例えば、データのパケット化やデータの連結等を行う。無線通信制御部２０は、レイヤ２以上のデータを取り扱うため、データの種別を判断することができる。そして、データの種別に応じて、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができる。レイヤ１のデータでは、データの種別を判断できないため、そのデータが秘匿処理されるべきデータであるか、又は、完全性保証処理されるべきデータであるかを判断することができない。

無線通信部３０は、通信路符号化部３１０とベースバンド変復調部３２０と無線部３３０とアンテナ３４を備えている。通信路符号化部３１０は、各通信路用の符号化部と復号化部を有している。符号化部として、誤り検出符号化部３１１と誤り訂正符号化部３１２と物理フォーマット変換部３１３を有している。また、復号化部として物理フォーマット変換部３１４、誤り訂正復号化部３１５、誤り検出部３１６を有している。ベースバンド変復調部３２０は、帯域の変調及び復調を行う。ベー

スバンド変復調部３２０は、ベースバンド変調部３２１とベースバンド復調部３２２を有している。無線部３３０は、ベースバンド帯域の信号を伝送帯域に変換もしくは伝送帯域の信号をベースバンド帯域に変換する。無線部３３０は、アップコンバータ３３１とダウンコンバータ３３２を有している。

秘匿・完全性保証処理部４０は、無線通信制御部２０に接続されている。秘匿・完全性保証処理部４０は、無線通信制御部２０からデータを受け取り、秘匿処理を行う。また、データの完全性保証処理を行う。秘匿・完全性保証処理部４０は、無線通信制御部２０から秘匿及び完全性保証処理のための制御信号９１を入力する。また、秘匿・完全性保証処理部４０は、無線通信制御部２０からレイヤ２以上の任意の階層における秘匿処理の対象となるデータ及び／又は完全性保証処理の対象となるデータ９２を入力する。秘匿・完全性保証処理部４０は、入力した制御信号９１に基づいてデータ９２に対して秘匿処理及び／又は完全性保証処理を行い、無線通信制御部２０に出力する。制御信号９１の中には、鍵や初期値や秘匿処理と完全性保証処理との選択等のパラメータが含まれている。

図４は、秘匿・完全性保証処理部４０の構成図である。

秘匿・完全性保証処理部４０は、ＩＦ部４１０と１つのモジュール４１１を有している。モジュール４１１は、秘匿処理と完全性保証処理を１つの同一の回路又は１つの同一のアルゴリズムで行うものである。秘匿処理を行うか、完全性保証処理を行うかは、制御信号９１により決定される。

ここで、秘匿処理とは、データを暗号化、或いは、復号化することをいう。また、完全性保証処理とは、データの改竄の有無を検証するために、データに対して認証子を付加する処理、或いは、認証子を再生して

比較することによりデータの改竄の有無を判定する処理のことをいう。

秘匿処理と完全性保証処理は、同一の回路又は同一のアルゴリズム、或いは、類似の回路又は類似のアルゴリズムを用いて行うことができるため、図４に示すように、秘匿処理と完全性保証処理を１つのモジュール４１１で行うことが可能である。図４に示す場合は、ハードウェアリソース及びソフトウェアリソースの削減が可能である。以下、モジュールとは、ハードウェアのみで実現されるもの、ソフトウェアのみで実現されるもの、ハードウェアとソフトウェアとの組み合わせで実現されるもののいずれかをいうものとする。

ここで、携帯電話機に用いられる秘匿処理と完全性保証処理との具体例について説明する。

図１４は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｓｅｃｔｉｏｎ　６．３．に示された図である。

図１５は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｆｉｇｕｒｅ　１６ｂ．に示された図である。

図１６は、ＡＲＩＢ　ＳＴＤ－Ｔ６３　３３．１０２，３Ｇ　Ｓｅｃｕｒｉｔｙ；Ｓｅｃｕｒｉｔｙ　Ａｒｃｈｉｔｅｃｔｕｒｅ，Ｆｉｇｕｒｅ　１６．に示された図である。

図１４は、無線回線上での暗号化方法を示している。図１４において、記号の意味は、以下の通りである。

ＣＫ：ｃｉｐｈｅｒ　ｋｅｙ（暗号鍵）

Ｆ８：データ秘匿用関数

ＩＫ：ｉｎｔｅｇｒｉｔｙ　ｋｅｙ（メッセージ認証鍵）

Ｆ９：データ完全性用関数

携帯電話事業者は、ｆ１～ｆ５という関数を使い、認証処理を実現している。この処理の中で生成したＣＫとＩＫと呼ぶ１２８ビットの暗号鍵を、データ秘匿用関数（ｆ８）とデータ完全性用関数（ｆ９）に渡している。

図１５は、無線回線上での暗号化方法を示している。図１５において、記号の意味は、以下の通りである。

ｆ８：データ秘匿用関数

ＣＫ：ｃｉｐｈｅｒ　ｋｅｙ（暗号鍵）

ＭＥＳＳＡＧＥ：ユーザー・データ及び信号情報など送信者が受信者に送りたい暗号化前の平文

ＣＯＵＮＴ－Ｃ：送受信の通算回数を示す数値データ。送受信のたびに１を加算する。

ＢＥＡＲＥＲ：論理チャネルを識別するためのビット

ＤＩＲＥＣＴＩＯＮ：暗号文の送信方向を区別するためのビット

ＬＥＮＧＴＨ：ＭＥＳＳＡＧＥ或いは暗号文のビット長

図１５に示すように、データ秘匿用関数ｆ８で作成した乱数列を基にデータ暗号化／復号化を行う。

図１６は、メッセージ認証子生成方法を示している。図１６において、記号の意味は、以下の通りである。

ｆ９：データ完全性用関数

ＩＫ：ｉｎｔｅｇｒｉｔｙ　ｋｅｙ（メッセージ認証鍵）

ＣＯＵＮＴ－Ｉ：送受信の通算回数を示す数値データ。送受信のたびに１を加算する。

ＭＥＳＳＡＧＥ：ユーザー・データ及び信号情報など送信者が受信者に送りたい暗号化前の平文

ＤＩＲＥＣＴＩＯＮ：暗号文の送信方向を区別するためのビット

ＦＲＥＳＨ：ユーザー毎に生成する乱数

ＭＡＣ－Ｉ：ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ ｆｏｒ ｉｎｔｅｇｒｉｔｙ（送信者が計算するメッセージ認証子）

ＸＭＡＣ－Ｉ：ｅｘｐｅｃｔｅｄ ｍｅｓｓａｇｅ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ ｆｏｒ ｉｎｔｅｇｒｉｔｙ（受信者が計算するメッセージ認証子）

図１６に示すように、受信者側で２つのメッセージ認証子を比較することによりデータの完全性がチェックできる。

次に、動作について説明する。

無線網内で端末とネットワーク間の暗号化通信を行うには、データをやり取りする前に二者間で一方が相手を正当であると、或いは、双方が通信相手として正当であると確認する認証（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）という処理が必要になる。

図１４に示すように、一連の認証処理で端末とネットワークの双方は、関数ｆ１～ｆ５と呼ぶ５つの関数を使う。この関数は、認証と並行して端末とネットワークの両方に、それぞれ１２８ビットの暗号鍵（ＣＫ＝ｃｉｐｈｅｒ ｋｅｙ）とメッセージ認証鍵（ＩＫ＝ｉｎｔｅｇｒｉｔｙ ｋｅｙ）を生成する。

これら２つの鍵は、相互に認証した端末とネットワークだけが同じものを持つことができ、後述するｆ８とｆ９との２つの関数で使われる。これら２つの鍵は通信毎に異なり、しかもそれらの間の規則性がない。そして、通信が終了した時点で廃棄される。

なお、この認証に必要な処理のメカニズム（プロトコル）は、標準化されているが、認証処理で用いられるｆ１～ｆ５の関数は標準化されておらず、オペレータが独自に決めることになっている。

認証処理が完了した後は、秘匿処理に用いられるデータ秘匿（ｄａｔａ　ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ）技術と完全性保証処理に用いられるデータ完全性（ｄａｔａ　ｉｎｔｅｇｒｉｔｙ）技術で、データのセキュリティを保っている。

１つ目のデータ秘匿技術は、無線ネットワーク上で音声を含むユーザー・データや信号情報を暗号化し、盗聴を防止する技術である。このデータ秘匿を実現するために、データ秘匿用関数（以下、ｆ８と呼ぶ）という関数を用いる。

図１５に示すデータを秘匿してやり取りする場合、送信者は認証の際に生成した暗号鍵（ＣＫ）を使う。更に、ｆ８には、ＣＫの他に、暗号化／復号化対象データのビット長（ＬＥＮＧＴＨ）、アップ／ダウンリンク（ＤＩＲＥＣＴＩＯＮ）、カウンタ（ＣＯＵＮＴ－Ｃ）、論理チャネル識別子（ＢＥＡＲＥＲ）を入力することで乱数列が生成される。

ここで、アップ／ダウンリンクとは、暗号文が端末から基地局へ送信されるのか、或いは、基地局から端末へ送信されるのかを区別するビットをいう。また、カウンタとは、送受信の通算回数を示すデータである。カウンタには、送受信のたびに決められた値を加算する。カウンタは、過去に送られた暗号文を後に送りつける攻撃を防ぐために用いられる。また、論理チャネルの識別子とは、暗号化を行う論理チャネルを識別するビットのことである。

生成した乱数列と暗号化したいデータ／信号情報との排他的論理和をとって暗号文を生成し、受信者に送信する。

ＣＫ以外のパラメータは、送信者から暗号化せずに受信者へ送付する。但し、ＣＫだけは認証処理の過程で受信者側でも同じものが生成されているため、送信する必要がない。

ＣＫ以外のパラメータが第三者に渡ったとしても、ＣＫが秘密であれ

ば暗号文を解読するための乱数列が生成できないため、元のメッセージの安全性は保たれる。

受信者側は、送られてきたパラメータと予め持っていたＣＫを使って乱数列を生成し、送られてきた暗号文と排他的論理和をとって、元のメッセージを復号する。

これは、ＩＳＯ／ＩＥＣ１０１１６で定義されたブロック暗号の利用モードの１つであるＯＦＢ（ｏｕｔｐｕｔ　ｆｅｅｄｂａｃｋ）モードの変形である。ＯＦＢモードは、暗号文に伝送路上で発生したノイズが混入しても、復号時点でそのノイズ部分を拡大することがないため、特に無線音声通信で採用される場合が多い。

２つ目のデータ完全性技術は、無線回線上の信号情報にメッセージ認証子（完全性認証子）を付加することで信号の情報の改竄の有無を検出する技術である。メッセージ認証技術とも呼ばれている。このデータ完全性をを実現するために、データ完全性用関数（以下、ｆ９と呼ぶ）を用いる。このｆ９のコア部分にもＦ８と同じ暗号アルゴリズムが用いられている。

まず、認証の際にメッセージ認証鍵生成関数ｆ４を使ってメッセージ認証鍵（ＩＫ）を生成し、ｆ９に渡す。図１６に示すように、ｆ９にメッセージ認証鍵の他、データ（ＭＥＳＳＡＧＥ）、アップ／ダウンリンク（ＤＩＲＥＣＴＩＯＮ）、カウンタ（ＣＯＵＮＴ－Ｃ）、ユーザー毎に生成する乱数（ＦＲＥＳＨ）を入力すると、メッセージ認証子（ＭＡＣ－Ｉ又はＸＭＡＣ－Ｉ）が生成される。

これらのパラメータも送信者から暗号化されないデータ・フォーマットのエリアに乗せて受信者へ送付される。これらのパラメータが第三者に渡っても、メッセージ認証鍵（ＩＫ）が秘密であれば、安全性は保たれるのはデータの秘匿の場合と同じである。

送信者は、このメッセージ認証子（ＭＡＣ－Ｉ）をデータに付加して、受信者へ送信する。受信者は同様に、ｆ９を使ってメッセージ認証子（ＸＭＡＣ－Ｉ）を計算する。ＭＡＣ－ＩとＸＭＡＣ－Ｉを比較し、同じであれば、改竄がなかったことを確認できる。

なお、改竄ありと検出された場合の処理の一例として、

（１）相手に再送信を要求し、再度受信したメッセージ認証子が正当かを確認する。

（２）続けて何回か改竄ありと検出した場合は、接続を切断するなどの対応をとる。

３Ｇｐｐ仕様（詳細は、ｈｔｔｐ：／／ｗｗｗ．３ｇｐｐ．ｏｒｇ／Ａｂｏｕｔ＿３ＧＰＰ／３ｇｐｐ．ｈｔｍを参照のこと）によると、暗号化／復号化モジュールは、図１５のように、入力された平文（暗号化されるデータ）を暗号文（暗号化されたデータ）に暗号化し出力する機能、また、暗号文を平文に復号化し出力する機能を持つ。３Ｇｐｐ仕様に基づくとすると、図３の制御信号９１の具体例は、上記ＣＯＵＮＴ／ＢＥＲＡＲＥＲ／ＤＩＲＥＣＴＩＯＮ／ＣＫ／ＬＥＮＧＴＨが該当する。

また、図３のデータ９２，９３の具体例としては、例えば、図２１に示すように、「ＭＡＣＳＤＵ」又は「ＲＬＣＰＤＵ（ｄａｔａｐａｒｔ）」となる。ここで、「ＲＬＣＰＤＵ（ｄａｔａｐａｒｔ）」とは、ＲＬＣＰＤＵの上位１Ｏｃｔもしくは２Ｏｃｔ（１バイトもしくは２バイト）を削除した部分（図２１の「ＤＡＴＡ　ＦＯＲ　ＣＩＰＨＥＲＩＮＧ」の部分）となる。「ＭＡＣＳＤＵ」又は「ＲＬＣＰＤＵ（ｄａｔａｐａｒｔ）」は、図１５のＭＥＳＳＡＧＥの一例である。また、ＭＡＣＳＤＵは、Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｓｅｒｖｉｃｅ　Ｄａｔａ　Ｕｎｉｔのことである。ＲＬＣＰＤＵは、Ｒａｄｉｏ

Ｌｉｎｋ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ Ｄａｔａ Ｕｎｉｔのことである。メッセージフローの各メッセージは、ＲＬＣＰＤＵから、ＲＬＣヘッダ削除後、レイヤ３において組み立てられたものとなる。

ＲＬＣＰＤＵにおいて、１Ｏｃｔもしくは２Ｏｃｔの秘匿対象外部分が存在するが、ＲＬＣＰＤＵ全てを秘匿・完全性保証処理部４０に入力し、秘匿・完全性保証処理部４０にて、１Ｏｃｔもしくは２Ｏｃｔ秘匿を行わないようにしている。その理由は、秘匿処理を行う全てのデータ単位（ＲＬＣＰＤＵ）から１Ｏｃｔもしくは２Ｏｃｔの秘匿対象外部分を取り除くため、１Ｏｃｔもしくは２Ｏｃｔのシフト処理を無線通信制御部２０において実行させることにより発生する無線通信制御部２０の負荷を低減するためである。

図５は、秘匿・完全性保証処理部４０の他の例を示す図である。

図５において特徴となる点は、秘匿処理部４２０と完全性保証処理部４３０を個別に設けた点である。秘匿処理部４２０の内部には、暗号化／復号化部４２１が設けられている。完全性保証処理部４３０の内部には、完全性認証子付加／完全性確認部４３１が設けられている。暗号化／復号化部４２１は、暗号化と復号化を１つの同一モジュールを用いて行う場合を示している。完全性認証子付加／完全性確認部４３１は、完全性認証子の付加と完全性の確認を１つの同一のモジュールで行う場合を示している。図５に示す場合は、暗号化と復号化が同じ関数であった場合及び完全性認証子付加と完全確認が同じ関数であった場合に、取り得る構成である。図５に示す場合は、図６に示す場合に比べ、ハードウェアリソース及びソフトウェアリソースの削減が可能である。

図６は、秘匿・完全性保証処理部４０の他の構成を示す図である。

図６の特徴は、秘匿処理部４２０において、暗号化部４２２と復号化部４２３を個別に設けた点である。また、完全性保証処理部４３０にお

いて、完全性認証子付加部４３２と完全性確認部４３３を個別に設けた点である。図６に示す場合は、暗号化と復号化が同じ又は違う関数であった場合及び完全性認証子付加と完全性確認が同じ又は違う関数であった場合に取る構成である。図６の場合は、暗号化、復号化、完全性認証子付加、完全性確認を個別に実行でき、送受信されるデータが同時並列に秘匿処理、或いは、完全性保証処理されるので、処理の高速化が可能である。

図７は、秘匿処理部４２０において、複数の暗号化部４２２と複数の復号化部４２３を設けた場合を示している。また、完全性保証処理部４３０において、複数の完全性認証子付加部４３２と複数の完全性確認部４３３を設けた場合を示している。無線端末（ＭＳ）１００が動作している場合に、複数のチャネルが同時に処理されなければならない場合がある。例えば、音声とファクシミリデータの２種類のデータが同時に伝送されるような場合には、少なくとも２チャネルのデータが同時に処理される必要がある。このような場合には、音声データを暗号化部１で暗号化し、ファクシミリデータを暗号化部２で暗号化することができる。また、復号する場合にも、同時に複数チャネルのデータを復号化することができる。暗号化部４２２と復号化部４２３と完全性認証子付加部４３２と完全性確認部４３３の数（図７では、ｎ個）は、全て同一である必要はなく、無線端末（ＭＳ）１００において同時に処理すべきチャネルの数に応じて各部分の数を決定すればよい。或いは、各チャネルに対応するのではなく、ある１つのチャネルに大量データの高速処理を行う必要が生じた場合に、その１つのチャネルに割り当てられた大量データを２つの暗号化部により処理するようにしても構わない。即ち、暗号化部４２２と復号化部４２３と完全性認証子付加部４３２と完全性確認部４３３の各部の数は、同時に処理すべきチャネルの数及び／又はデータ

量により決定すればよい。

また、暗号化部４２２の最大数と復号化部４２３の最大数は異なってもよい。

また、完全性認証子付加部４３２の最大数と完全性確認部４３３の最大数は異なってもよい。

図８は、秘匿処理部４２０に複数の暗号化／復号化部４２１を設けた場合を示している。また、完全性保証処理部４３０に複数の完全性認証子付加／完全性確認部４３１を設けた場合を示している。

図８は、図５に示す暗号化／復号化部４２１と完全性認証子付加／完全性確認部４３１を複数にしたものである。図８に示す場合は、暗号化と復号化が同じ関数であった場合に、複数のチャネルに対応して複数の暗号化／復号化部４２１を設けた場合を示している。同様に、完全性認証子付加と完全性確認が同じ関数であった場合に、複数のチャネルに対応して完全性認証子付加／完全性確認部４３１を複数設けた場合を示している。図８の場合は、図７の場合に比べて、ハードウェアリソース及びソフトウェアリソースの削減を行うことが可能である。

図４から図８においては、秘匿・完全性保証処理部４０が秘匿処理部４２０と完全性保証処理部４３０とを両方備えている場合を示したが、秘匿・完全性保証処理部４０が秘匿処理部４２０又は完全性保証処理部４３０のいずれか片方だけ備えている場合でもよい。秘匿・完全性保証処理部４０が秘匿処理部４２０又は完全性保証処理部４３０の一方だけ備えている場合は、他方の処理は、無線通信制御部２０が行えばよい。

実施の形態２.

図９は、無線端末（ＭＳ）１００の他の例を示す構成図である。

図９が図３と異なる点は、端末ＩＦ部１０と秘匿・完全性保証処理部４０との間でデータの入出力が行われる点である。また、無線通信部３

０と秘匿・完全性保証処理部４０との間でデータの入出力が行われる点である。図９において、非透過データ９７は、パケットデータ等の非透過データである。また、透過データ９５，９６は、音声データや非制限デジタルデータ等の透過データである。透過データとは、ＯＳＩで定義されているあるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータが一切変更されないデータをいう。一方、非透過データとは、あるレイヤ、或いは、あるレイヤのサブレイヤにおいて、入力から出力まで、そのデータのフォーマット変換処理等の何等かのデータ処理が必要なデータをいう。例えば、レイヤ２のＲＬＣ（Ｒａｄｉｏ　Ｌｉｎｋ　Ｃｏｎｔｒｏｌ）サブレイヤにおいて、ＳＤＵ（Ｓｅｒｖｉｃｅ　Ｄａｔａ　Ｕｎｉｔ）とＰＤＵ（Ｐｒｏｔｏｃｏｌ　Ｄａｔａ　Ｕｎｉｔ）とが異なる場合は、そのデータは非透過データであり、レイヤ２のＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）サブレイヤにおいて、ＳＤＵとＰＤＵが同一の場合、そのデータは透過データである。図９に示す場合は、無線通信部３０との間で入出力されるレイヤ１のデータに対して何等処理を行うことなく、端末ＩＦ部１０に引き渡すことができるデータ、例えば、音声データを、透過データとしている。一方、無線通信部３０から出力されるレイヤ１のデータに対して何等かの処理を行わなければならないデータ、例えば、パケットデータを、非透過データとしている。

図９の透過データ９５，９６の具体例は、前述した通り、音声データや非制限デジタルデータであるが、それぞれのデータは、レイヤ１とレイヤ２の間に定義される単位（Ｔｒａｎｓｐｏｒｔ　Ｂｌｏｃｋ）に分割されたものであり、これらＴｒａｎｓｐｏｒｔ　Ｂｌｏｃｋに分割されたデータは透過データであるため、前述の通り、ＭＡＣＰＤＵ（かつ、ＭＡＣＳＤＵ）と等価であるため、Ｔｒａｎｓｐｏｒｔ　Ｂｌｏｃｋ

に分割されたデータそれぞれが、秘匿の単位と同一となる。

また、音声データ等は、ユーザーデータであり、ユーザーデータは、ＲＬＣサブレイヤにおいても透過データであることから、この伝送形態をシリアルインタフェースとして、ＡＲＩＢ規定のＭＴ（Ｍｏｂｉｌｅ Ｔｅｒｍｉｎａｌ）－ＴＡ（Ｔａｒｍｉｎａｌ Ａｄａｐｔｏｒ）Ｉ／Ｆ（図２２，図２３）とすると、ＭＴ－ＴＡ Ｉ／Ｆのシリアルフォーマットに対しそのまま、秘匿を施すことが可能な伝送形態となる。

また、図９の非透過データ９７の具体例は、前述した通り、パケットデータやシグナリングのためのデータであるが、各データは、レイヤ１とレイヤ２との間に定義される単位（Ｔｒａｎｓｐｏｒｔ Ｂｌｏｃｋ）に分割されたものである。

図９に示す秘匿・完全性保証処理部４０は、無線通信制御部２０との間で非透過データに対して秘匿処理と完全性保証処理を選択的に行うとともに、端末ＩＦ部１０と無線通信部３０との間で入出力される透過データに対して、例えば、秘匿処理を必ず行うものである。秘匿・完全性保証処理部４０は、透過データに対しては完全性保証処理を行わない。もし、透過データのなかに秘匿処理を行いたくないものがある場合には、無線通信制御部２０は、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部４０に入力させず無線通信制御部２０に入力させればよい。或いは、その秘匿処理を行いたくない透過データを秘匿・完全性保証処理部４０に入力させるが、無線通信制御部２０からの制御信号を用いてその透過データに秘匿処理を行わせないようにしてもよい。

図１０は、秘匿・完全性保証処理部４０の構成図である。

図１０において、図５と異なる点は、新たに秘匿処理部４６０が設けられた点である。秘匿処理部４６０には、暗号化部４６２と復号化部４６３が設けられている。暗号化部４６２は、端末ＩＦ部１０からの透過

データ９５を入力し、入力したデータを暗号化し、透過データ９６として無線通信部３０へ出力する。一方、復号化部４６３は、無線通信部３０から透過データ９６を入力し、復号化し、透過データ９５として端末ＩＦ部１０へ出力する。秘匿処理部４６０のこれらの処理は、ＩＦ部４１０からの制御信号９９に基づいて行われる。制御信号９９は、制御信号９１から生成された制御信号である。従って、秘匿処理部４６０は、無線通信制御部２０からの制御信号に基づいて秘匿処理を行うことになる。図１０において、データ９２は、バスを介したパラレルインタフェースを用いて入出力される。一方、透過データ９５と９６は、シリアルインタフェースを介して秘匿処理部４６０に対して入出力される。このように、図１０は、秘匿・完全性保証処理部４０がパラレルインタフェースとシリアルインタフェースの２系統の入出力インタフェースを備えている場合を示している。

図１１は、図７に示した秘匿・完全性保証処理部４０の構成に秘匿処理部４６０を付加した場合を示している。図１１に示すような秘匿処理部４６０の構成は、図１２に示すように、暗号化部又は復号化部がキーストリームを発生させ、シリアルデータと排他的論理和をとる場合に有効な構成である。

図１１は、透過データ９５，９６がシリアルインタフェースを介して秘匿処理部４６０に入出力される場合であって、かつ、そのシリアルインタフェースを介して入出力されるシリアルデータに、複数チャネルのデータが多重化されている場合を示している。例えば、チャネル１のデータの次にチャネル２のデータがシリアルデータとして入力された場合、チャネル１に対応する暗号化部１からキーストリームを発生させデータ多重部４８１に出力し、チャネル２に対応する暗号化部２からキーストリームを発生させデータ多重部４８１に出力し、データ多重部４８１

において、これらのキーストリームを入力されるデータ９５のデータ系列と同じフォーマットに多重する。この多重したキーストリームと入力されるデータ９５のデータ系列との排他的論理和を排他的論理和回路４８３により演算する。秘匿処理部４６０のこれらの動作は制御信号９９に基づいて、即ち、無線通信制御部２０から送られてきた制御信号９１に基づいて行われる。図１１の構成によれば、シリアルデータの遅延が排他的論理和回路４８３の演算のみで済み、高速な処理を行うことが可能である。

図１３は、図１０の秘匿処理部４２０と秘匿処理部４６０とをあわせて１つの秘匿処理部４７０とした場合を示している。

秘匿処理部４７０は、パラレルインタフェースから入出力されるデータ９２とシリアルインタフェースから入出力されるデータ９５，９６の両方を処理する。秘匿処理部４７０は、秘匿処理部４２０と秘匿処理部４６０を１つにまとめたものであるため、ハードウェアリソースの削減が可能である。秘匿処理部４７０における透過データと非透過データの処理動作のスイッチングは、制御信号９９、即ち、無線通信制御部２０から出力された制御信号９１に基づいて行われる。

前述した秘匿・完全性保証処理部４０は、ハードウェアで構成することができる。例えば、ＦＰＧＡやカスタムＬＳＩで実現することができる。また、秘匿・完全性保証処理部４０は、ソフトウェアプログラムで実現することもできる。秘匿・完全性保証処理部４０がソフトウェアプログラムで実現される場合、ソフトウェアプログラムは無線通信制御部２０にあるＣＰＵにより実行されることになる。

また、秘匿・完全性保証処理部４０は、ハードウェアとソフトウェアの組み合わせにより実現することができる。例えば、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）とそのＤＳＰにより実行

されるマイクロプログラムやファームウェアプログラムにより実現することができる。

以下、図１７から図２０を用いて、具体例を説明する。

図１７は、暗号化／復号化部４２１の中で用いられる暗号化モジュール５１（又は復号化モジュール７１）の構成図である。

暗号化モジュール５１は、鍵スケジュール部５１１とデータランダマイズ部５１２を有している。鍵スケジュール部５１１は、１つの鍵Ｋを入力してｎ個の拡大鍵$ExtK_1$～$ExtK_n$を生成する。データランダマイズ部５１２は、関数ＦとＸＯＲ回路とにより乱数を発生させる。関数Ｆは、拡大鍵を入力して非線形データ変換を行う。

暗号モジュール５１においては、例えば、

（１）ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、又は、

（２）国際公開番号ＷＯ９７／９７０５（米国特許出願番号０８／８３６４０）に開示されたブロック暗号アルゴリズムであるＭＩＳＴＹ、又は、

（３）上記ブロック暗号アルゴリズムＭＩＳＴＹをベースとした６４ビットブロック暗号であり、次世代携帯電話用国際標準暗号（ＩＭＴ２０００）として採用されることが決定されたブロック暗号アルゴリズムであるＫＡＳＵＭＩ、又は、

（４）日本特許出願番号２０００－６４６１４（出願日２０００年３月９日）に記載されたブロック暗号アルゴリズムであるＣａｍｅｌｌｉａ

などのブロック暗号アルゴリズムを用いることができる。また、復号モジュール７１においても、ＤＥＳ、ＭＩＳＴＹ、ＫＡＳＵＭＩ又はＣａｍｅｌｌｉａなどのブロック暗号アルゴリズムを用いることができる。

図１８は、前述した秘匿・完全性保証処理部４０の実装形式を示す図である。

図１８は、ＦＰＧＡ又はＩＣ又はＬＳＩの中に前述した秘匿・完全性保証処理部４０が実現されている場合を示している。即ち、前述した秘匿・完全性保証処理部４０は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

図１９は、前述した秘匿・完全性保証処理部４０をソフトウェアで実現する場合を示している。

前述した秘匿・完全性保証処理部４０は、暗号化プログラム４７で実現することができる。暗号化プログラム４７は、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）４２（記録媒体の一例）に記憶されている。暗号化プログラム４７は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）又はフレキシブルディスク又は固定ディスク等の他の記録媒体に記録されていてもよい。また、暗号化プログラム４７は、サーバコンピュータからダウンロードされてもよい。暗号化プログラム４７は、サブルーチンとして機能する。暗号化プログラム４７は、ＲＡＭ４５に記憶されたアプリケーションプログラム４６からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム４７は、割り込み制御部４３で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ５５は、ＲＡＭ４５の一部であっても構わない。アプリケーションプログラム４６、暗号化プログラム４７は、ＣＰＵ４１により実行されるプログラムである。

図２０は、無線通信制御部２０で動作するアプリケーションプログラム４６が暗号化プログラム４７を呼び出すメカニズムを示している。

アプリケーションプログラム４６は、鍵Ｋとイニシャルバリュー ＩＶ

と平文Mと暗号文Cをパラメータにして暗号化プログラム４７を呼び出す。暗号化プログラム４７は、鍵Kとイニシャルバリュー ＩＶと平文Mを入力し、暗号文Cを返すものである。暗号化プログラム４７と復号プログラムが同一のときは、鍵Kとイニシャルバリュー ＩＶと暗号文Cと平文Mをパラメータにして暗号化プログラム４７を呼び出す。

また、図示しないが、暗号化プログラム４７は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム４７を実現しても構わない。

図１８，図１９，図２０は、主として、暗号化の場合を説明したが、復号化でも同様の方式で実現できる。

図１８及び図１９に示したような暗号化形態及び復号化形態は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号化する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号化する場合に、或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号化するデータの数に比べて暗号化復号化する装置の数が少ない場合に、前述した実施の形態の暗号化、復号化が非常に有効である。例えば、多くのクライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しなければならない基地局や回線コントローラなどに、前述した暗号化方

式や復号化方式が非常に有効である。

また、前述した例においては、無線通信制御部２０と秘匿・完全性保証処理部４０がバスを介したパラレルインタフェースでつながれている場合を示したが、シリアルインタフェースを用いても構わない。また、端末ＩＦ部１０と秘匿・完全性保証処理部４０及び無線通信部３０と秘匿・完全性保証処理部４０がシリアルインタフェースで接続される場合を示したが、より高速な処理を行うためには、シリアルインタフェースではなく、パラレルインタフェースを用いても構わない。

また、図９，図１０においては、秘匿処理部４６０を秘匿・完全性保証処理部４０の内部に設ける場合を示したが、秘匿処理部４６０を秘匿・完全性保証処理部４０から外部に独立させて、秘匿処理部４６０を端末ＩＦ部１０と無線通信部３０との間に設けてもよい。

産業上の利用可能性

以上のように、前述した実施の形態によれば、レイヤ１（物理層）において秘匿処理を行わないように、レイヤ２以上の階層において秘匿処理及び完全性保証処理を行うようにしたので、データの種別に応じて秘匿処理の可否及び完全性保証処理の可否を決定することができる。

例えば、透過データに対しては秘匿処理のみを行い、非透過データに対して秘匿処理と完全性保証処理の両方を行うことが可能になる。或いは、非透過データであっても秘匿処理と完全性保証処理とをそれぞれ行ったり、行わなかったり選択することが可能になる。

また、上記実施の形態によれば、秘匿・完全性保証処理部の内部にチャネルの数やデータ量に応じて複数の秘匿処理部と複数の完全性保証処理部を設けているので、同時並列処理による高速データ処理が可能となる。

請求の範囲

1．データを入力する端末インタフェース部と、

端末インタフェース部が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

無線通信制御部から出力されたデータを入力して変調し送信する無線通信部と

を備えたことを特徴とする無線通信装置。

2．上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて端末インタフェース部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを無線通信部に出力することを特徴とする請求項1記載の無線通信装置。

3．上記端末インタフェース部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを端末インタフェース部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを端末インタフェース部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする請求項2記載の無線通信装置。

4．上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする請求項１記載の無線通信装置。

5．上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項２記載の無線通信装置。

6．上記秘匿・完全性保証処理部は、

入力したデータを暗号化する暗号化部を有する秘匿処理部と、

入力したデータに対して完全性認証子を付加する完全性認証子付加部を有する完全性保証処理部と

を備えたことを特徴とする請求項１記載の無線通信装置。

7．上記秘匿処理部は、複数の暗号化部を有することを特徴とする請求項６記載の無線通信装置。

8．上記完全性保証処理部は、複数の完全性認証子付加部を有することを特徴とする請求項６記載の無線通信装置。

9．上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する１つのモジュールであり、その１つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする請求項６記載の無線通信装置。

１０．データを受信して復調する無線通信部と、

無線通信部により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御部と、

無線通信制御部から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘

匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御部へ出力する秘匿・完全性保証処理部と、

無線通信制御部により処理されたデータを入力して出力する端末インタフェース部と

を備えたことを特徴とする無線通信装置。

１１．上記秘匿・完全性保証処理部は、

無線通信制御部から制御信号を入力し、入力した制御信号に基づいて無線通信部からデータを選択的に入力するとともに、

入力したデータに対して秘匿処理を行い、

秘匿処理したデータを端末インタフェース部に出力することを特徴とする請求項１０記載の無線通信装置。

１２．上記無線通信部は、透過データと非透過データとを出力し、

上記無線通信制御部は、非透過データを無線通信部から入力してプロトコルに基づいて秘匿・完全性保証処理部に処理させるとともに、透過データを無線通信部から秘匿・完全性保証処理部に入力させて秘匿処理させることを特徴とする請求項１１記載の無線通信装置。

１３．上記秘匿・完全性保証処理部は、無線通信制御部とパラレルインタフェースで接続されていることを特徴とする請求項１０記載の無線通信装置。

１４．上記秘匿・完全性保証処理部は、端末インタフェース部とシリアルインタフェースで接続され、かつ、無線通信部とシリアルインタフェースで接続されることを特徴とする請求項１１記載の無線通信装置。

１５．上記秘匿・完全性保証処理部は、

入力したデータを復号化する復号化部を有する秘匿処理部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部を有する完全性保証処理部と

を備えたことを特徴とする請求項１０記載の無線通信装置。

１６．上記秘匿処理部は、複数の復号化部を有することを特徴とする請求項１５記載の無線通信装置。

１７．上記完全性保証処理部は、複数の完全性確認部を有することを特徴とする請求項１５記載の無線通信装置。

１８．上記秘匿処理部と完全性保証処理部とは、無線通信制御部から制御信号とデータとを入力する１つのモジュールであり、その１つのモジュールは、入力した制御信号に基づいて、入力したデータに対して少なくとも上記秘匿処理部と完全性保証処理部とのいずれかの処理を実行することを特徴とする請求項１５記載の無線通信装置。

１９．データを無線通信する無線通信装置において、

データを入出力する端末インタフェース部と、

プロトコルに基づいてデータの処理をする無線通信制御部と、

データを無線通信する無線通信部と、

端末インタフェース部と無線通信制御部と無線通信部との三者間に設けられ、無線通信制御部との間でデータに対して少なくともデータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース部から無線通信部へのデータを暗号化するとともに無線通信部から端末インタフェース部へのデータを復号する秘匿・完全性保証処理部と

を備えたことを特徴とする無線通信装置。

２０．上記秘匿・完全性保証処理部は、

入力したデータに対して秘匿処理を行う秘匿処理部と、

入力したデータに対して完全性保証処理を行う完全性保証処理部とを個別に備えたことを特徴とする請求項１９記載の無線通信装置。

２１．上記秘匿処理部は、

端末インタフェース部から無線通信部へのデータを暗号化する暗号化部と、

無線通信部から端末インタフェース部へのデータを復号化する復号化部とを個別に有することを特徴とする請求項１９記載の無線通信装置。

２２．上記完全性保証処理部は、

入力したデータに対して完全性保証処理を行う完全性認証子を付加する完全性認証子付加部と、

入力したデータに付加された完全性認証子を用いて入力したデータの完全性を確認する完全性確認部と

を個別に有することを特徴とする請求項１９記載の無線通信装置。

２３．上記通信装置は、携帯型移動電話機であることを特徴とする請求項１９記載の無線通信装置。

２４．上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項６記載の無線通信装置。

２５．上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項１５記載の無線通信装置。

２６．上記秘匿処理部と上記完全性保証処理部とは、同一の暗号アルゴリズムを用いていることを特徴とする請求項２０記載の無線通信装置。

２７．上記無線通信装置は、携帯電話機であることを特徴とする請求項１記載の無線通信装置。

２８．上記無線通信装置は、携帯電話機であることを特徴とする請求項１０記載の無線通信装置。

２９．上記無線通信装置は、携帯電話機であることを特徴とする請求項１９記載の無線通信装置。

３０．上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項１記載の無線通信装置。

３１．上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項１０記載の無線通信装置。

３２．上記無線通信装置は、無線端末との間でデータの送受信をする無線局であることを特徴とする請求項１９記載の無線通信装置。

３３．上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項３０記載の無線通信装置。

３４．上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項３１記載の無線通信装置。

３５．上記無線局は、無線基地局と無線制御局とのいずれかであることを特徴とする請求項３２記載の無線通信装置。

３６．データを入力する端末インタフェース工程と、

端末インタフェース工程が入力したデータを入力し、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを暗号化する秘匿処理とデータの改竄を検出するための完全性認証子を生成する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

無線通信制御工程から出力されたデータを入力して変調し送信する無線通信工程と

を備えたことを特徴とする無線通信方法。

３７．データを受信して復調する無線通信工程と、

無線通信工程により復調されたデータを入力して、プロトコルに基づいてデータを処理して出力する無線通信制御工程と、

無線通信制御工程から制御信号とデータとを入力し、入力した制御信号に基づいて、入力したデータに対して少なくともデータを復号化する秘匿処理とデータの改竄を検証する完全性保証処理とのいずれかの処理を行い、処理したデータを無線通信制御工程へ出力する秘匿・完全性保証処理工程と、

無線通信制御工程により処理されたデータを入力して出力する端末インタフェース工程と

を備えたことを特徴とする無線通信方法。

３８．データを無線通信する無線通信方法において、

データを入出力する端末インタフェース工程と、

プロトコルに基づいてデータの処理をする無線通信制御工程と、

データを無線通信する無線通信工程と、

端末インタフェース工程と無線通信制御工程と無線通信工程との三者間に設けられ、無線通信制御工程との間でデータに対して少なくともデータを暗号化復号化する秘匿処理とデータの改竄を検出する完全性保証処理とのいずれかの処理を行い、端末インタフェース工程から無線通信工程へのデータを暗号化するとともに無線通信工程から端末インタフェース工程へのデータを復号する秘匿・完全性保証処理工程と

を備えたことを特徴とする無線通信方法。

図 1

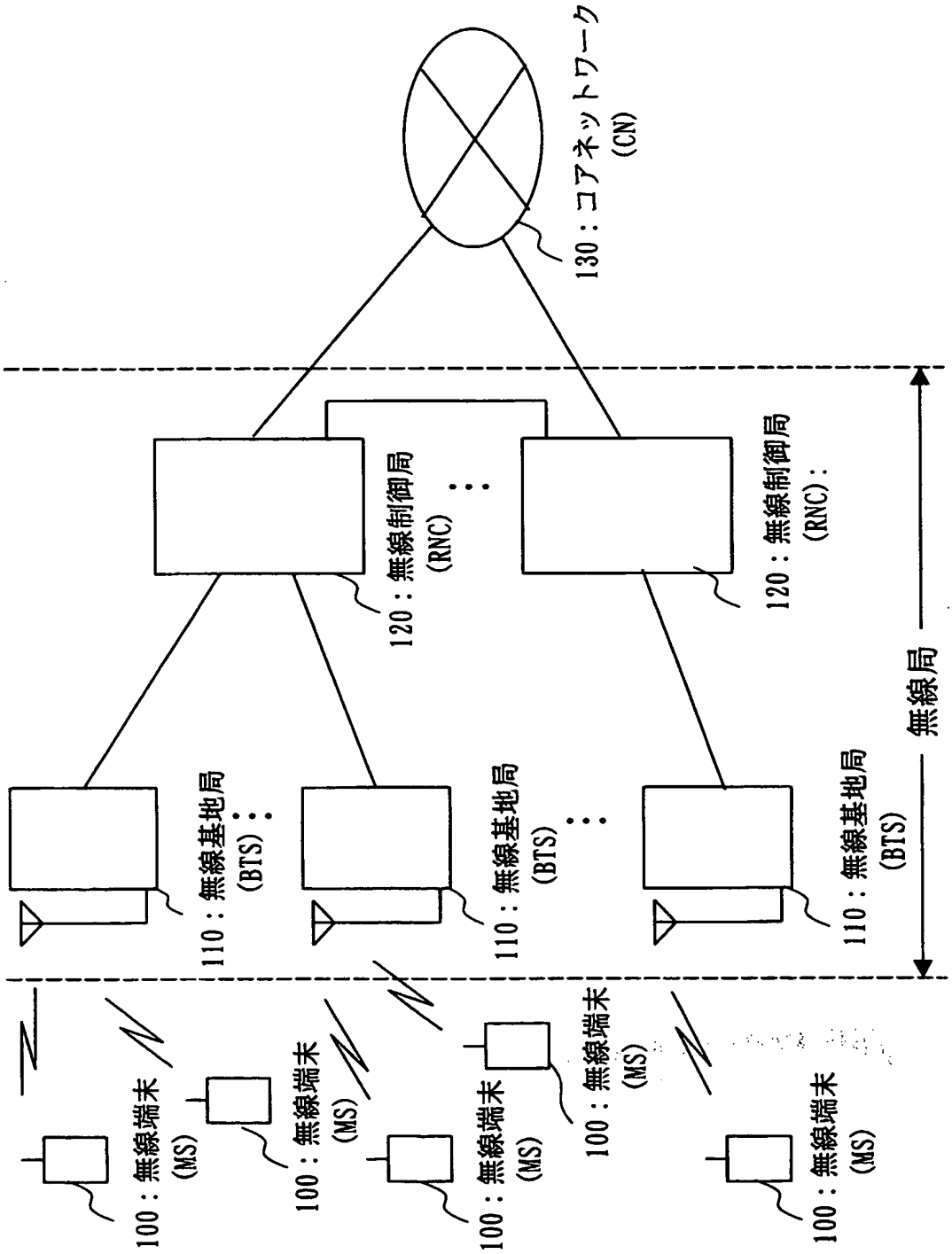

130：コアネットワーク
(CN)
120：無線制御局
(RNC)
120：無線制御局
(RNC)
110：無線基地局
(BTS)
110：無線基地局
(BTS)
110：無線基地局
(BTS)
無線局
100：無線端末
(MS)
100：無線端末
(MS)
100：無線端末
(MS)
100：無線端末
(MS)
100：無線端末
(MS)

図 2

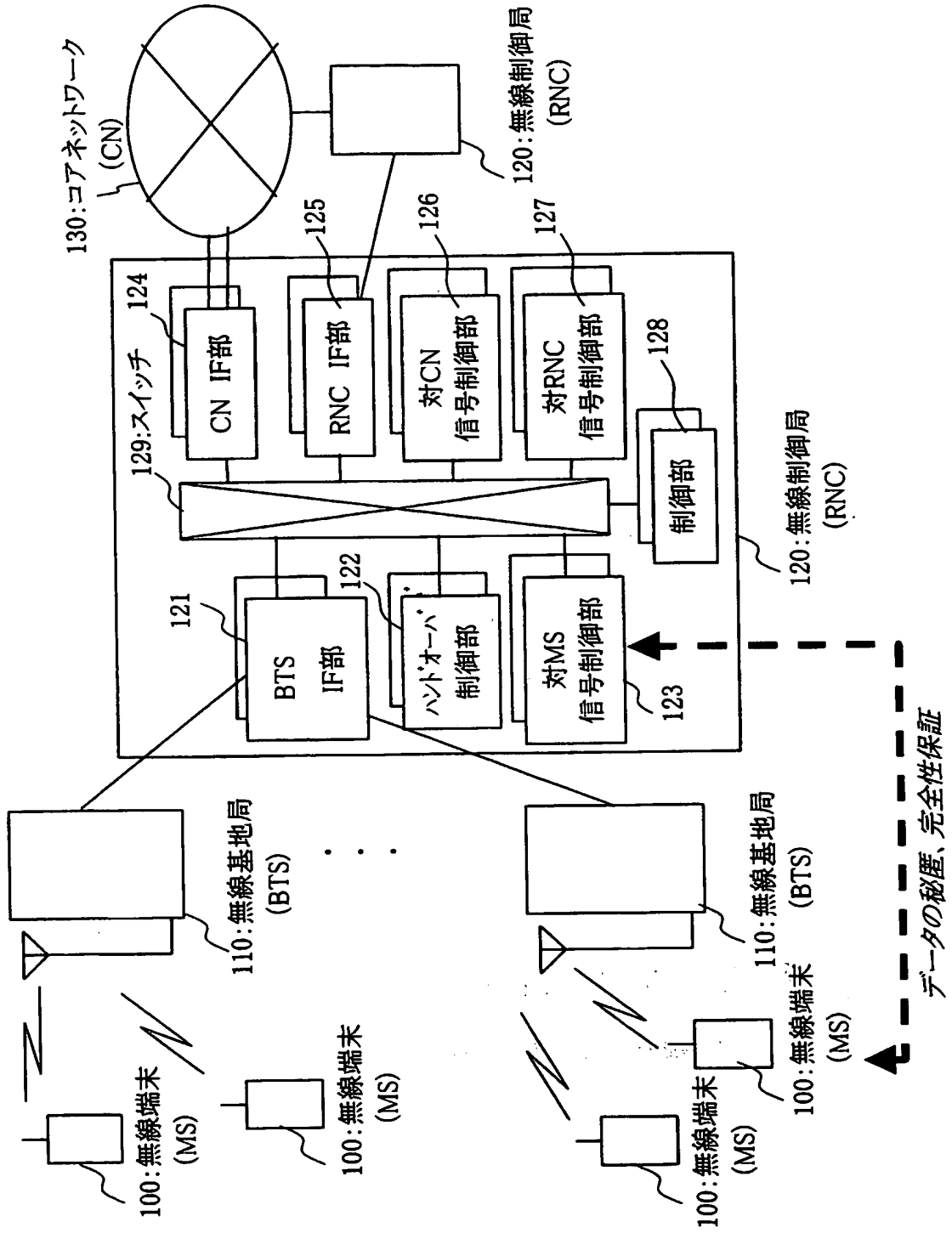

130:コアネットワーク (CN)
120:無線制御局 (RNC)
129:スイッチ
124
CN IF部
125
RNC IF部
126
対CN 信号制御部
127
対RNC 信号制御部
128
制御部
121
BTS IF部
122
ハンドオーバ 制御部
対MS 信号制御部
123
110:無線基地局 (BTS)
100:無線端末 (MS)
データの秘匿、完全性保証

図 3

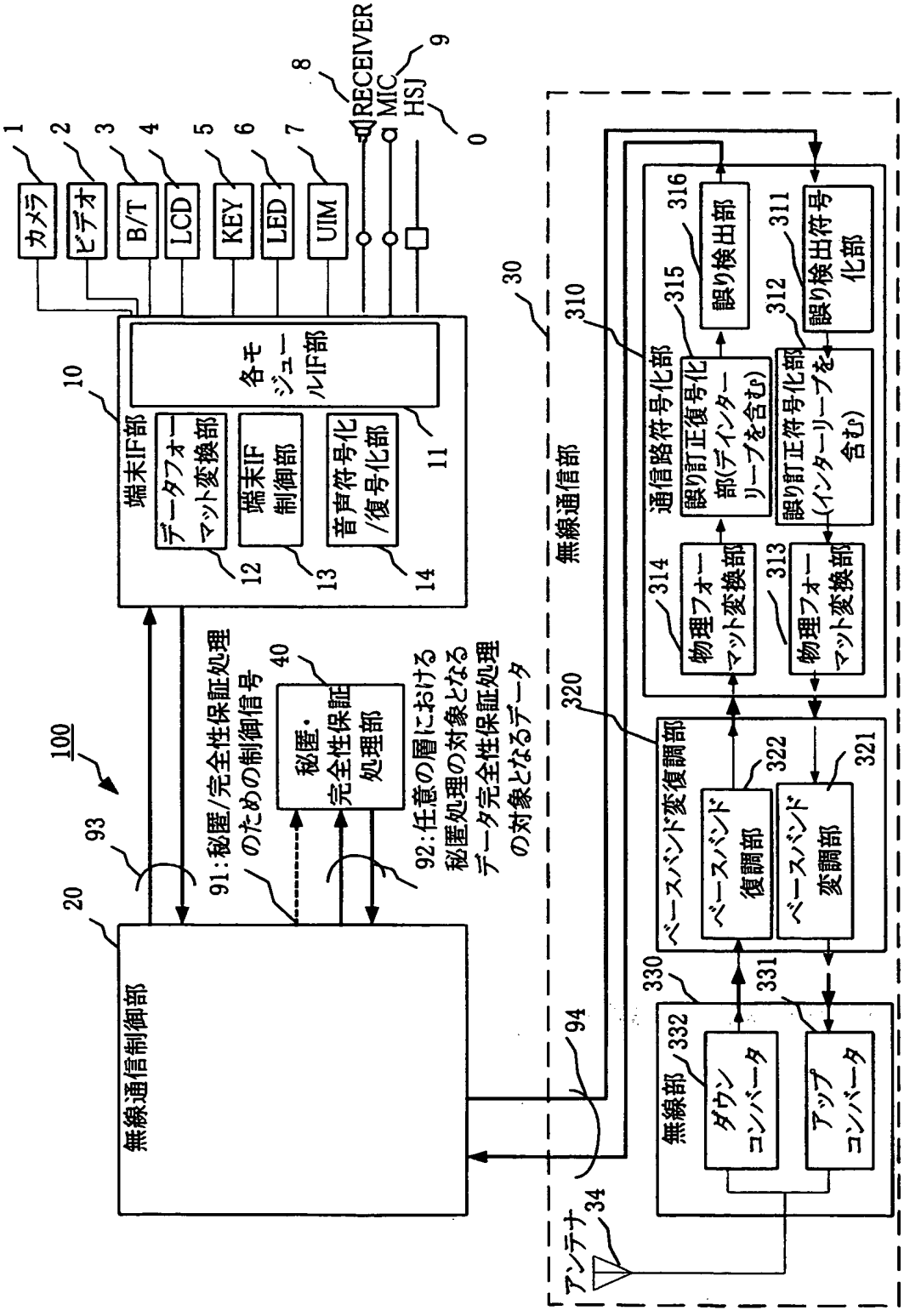

1
2
3
4
5
6
7
8
9
0
カメラ
ビデオ
B/T
LCD
KEY
LED
UIM
RECEIVER
MIC
HSJ
10
端末IF部
データフォーマット変換部
端末IF制御部
各モジュールIF部
音声符号化/復号化部
12
13
14
11
100
20
無線通信制御部
93
91:秘匿/完全性保証処理のための制御信号
40
秘匿・完全性保証処理部
92:任意の層における秘匿処理の対象となるデータ完全性保証処理の対象となるデータ
30
無線通信部
310
320
94
通信路符号化部
誤り訂正復号化部(デインターリーブを含む)
誤り検出部
315
316
誤り訂正符号化部(インターリーブを含む)
誤り検出符号化部
312
311
物理フォーマット変換部
物理フォーマット変換部
314
313
ベースバンド変復調部
ベースバンド復調部
ベースバンド変調部
322
321
330
無線部
ダウンコンバータ
アップコンバータ
332
331
アンテナ
34

図 4

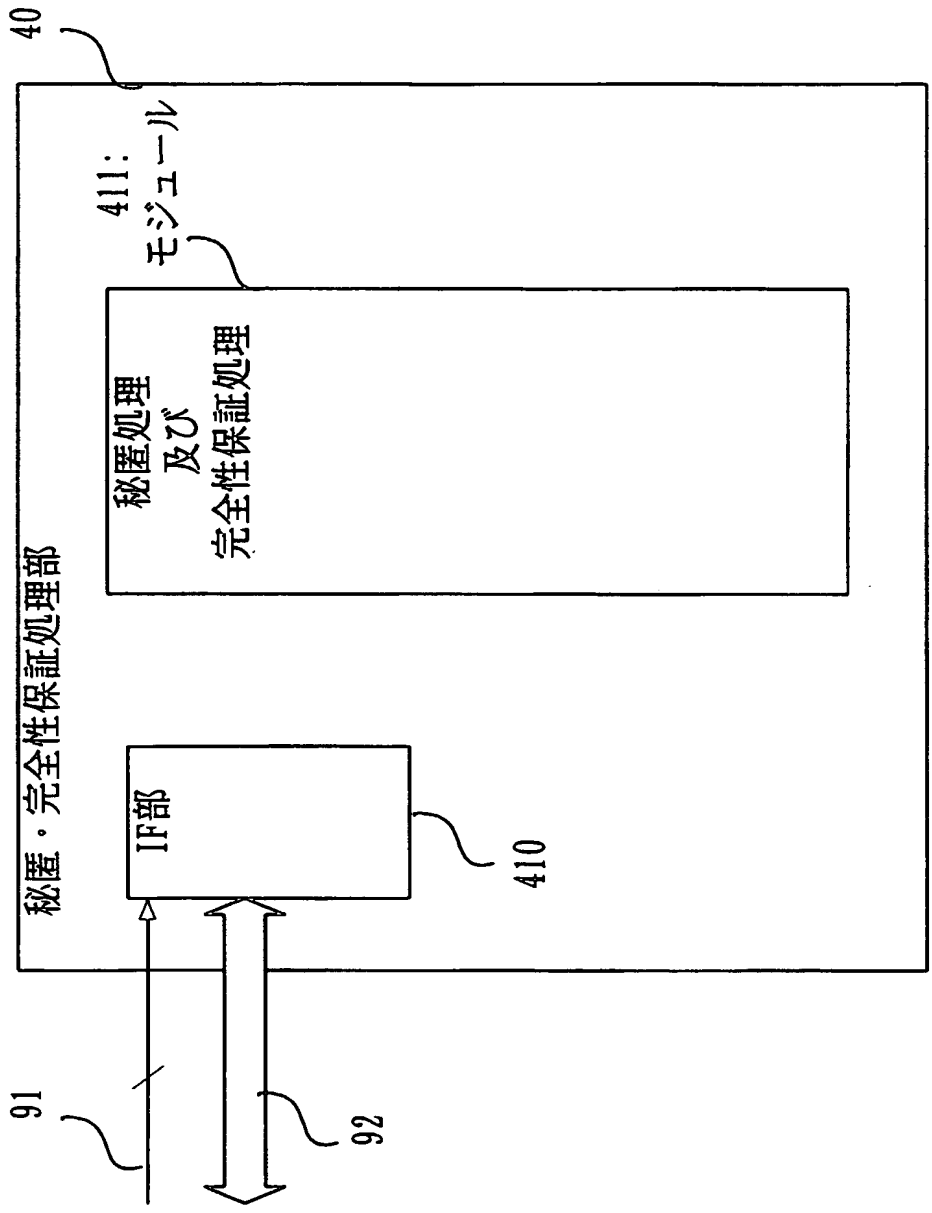


図 5

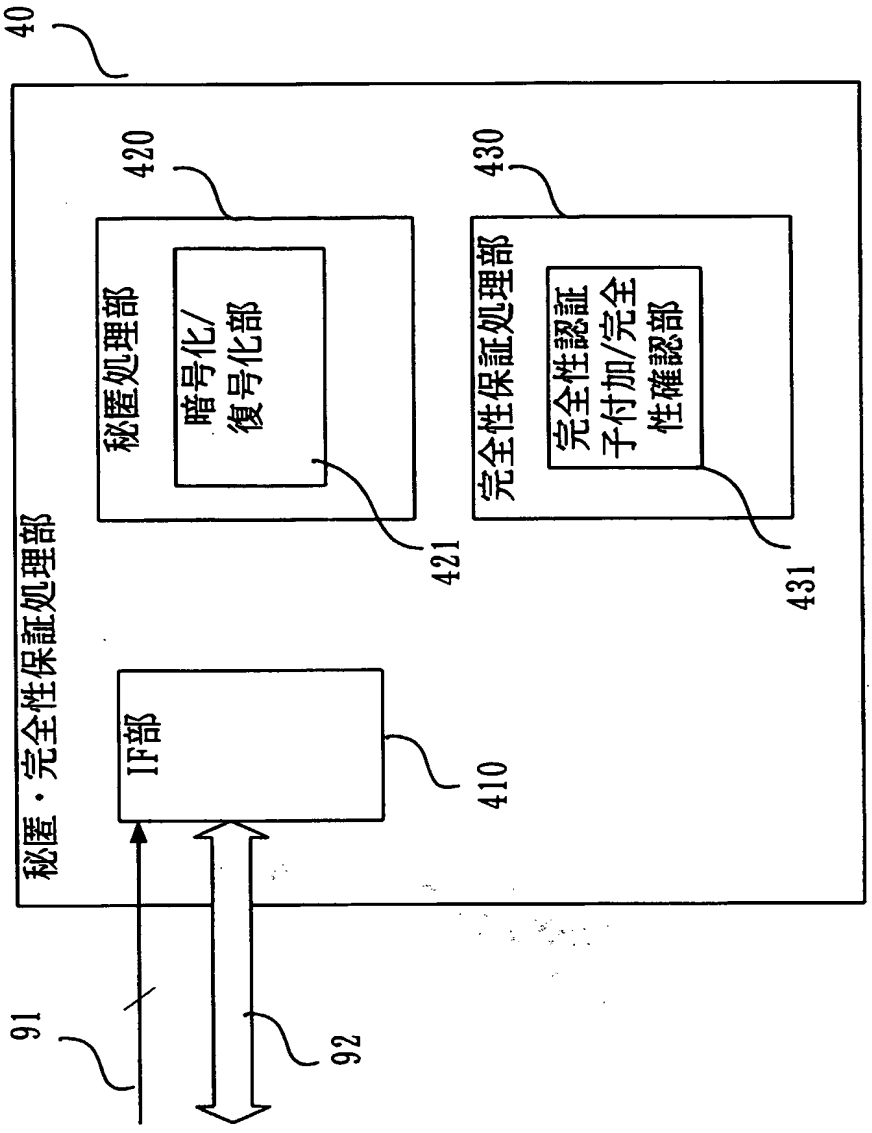

40
秘匿・完全性保証処理部
IF部
410
秘匿処理部
420
暗号化/
復号化部
421
完全性保証処理部
430
完全性認証
子付加/完全
性確認部
431
91
92

図 6

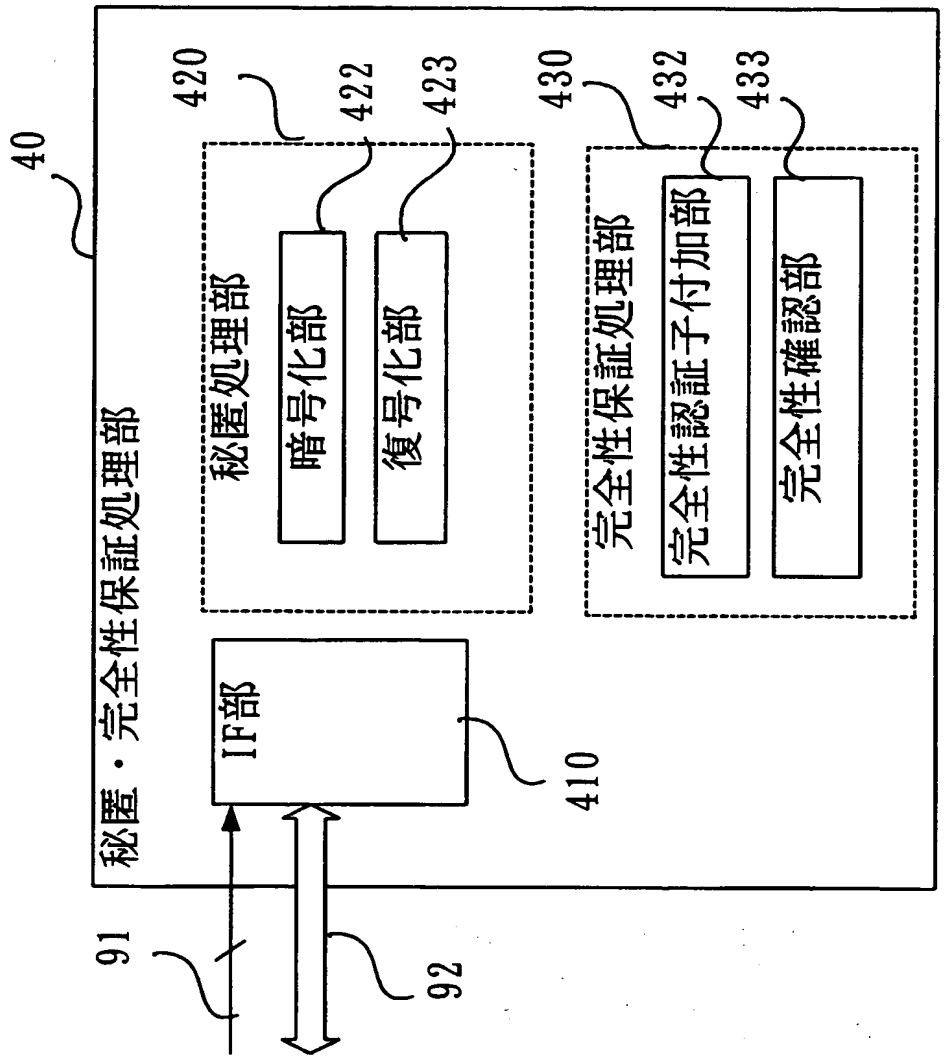

40
秘匿・完全性保証処理部
420
秘匿処理部
422
暗号化部
423
復号化部
430
完全性保証処理部
432
完全性認証子付加部
433
完全性確認部
IF部
410
91
92

図 7

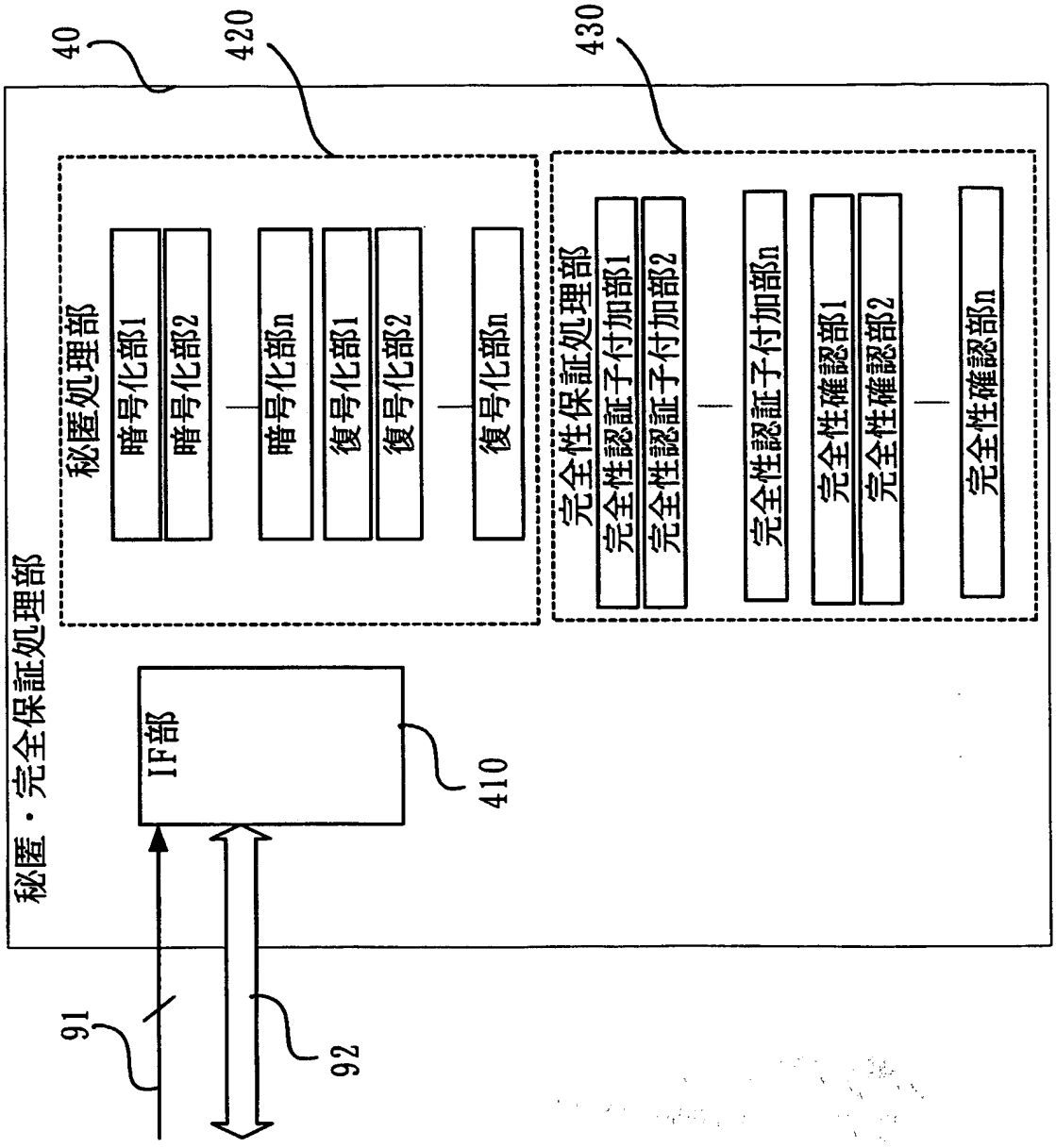

40
420
430
秘匿・完全保証処理部
秘匿処理部
暗号化部1
暗号化部2
暗号化部n
復号化部1
復号化部2
復号化部n
完全性保証処理部
完全性認証子付加部1
完全性認証子付加部2
完全性認証子付加部n
完全性確認部1
完全性確認部2
完全性確認部n
IF部
410
91
92

図 8

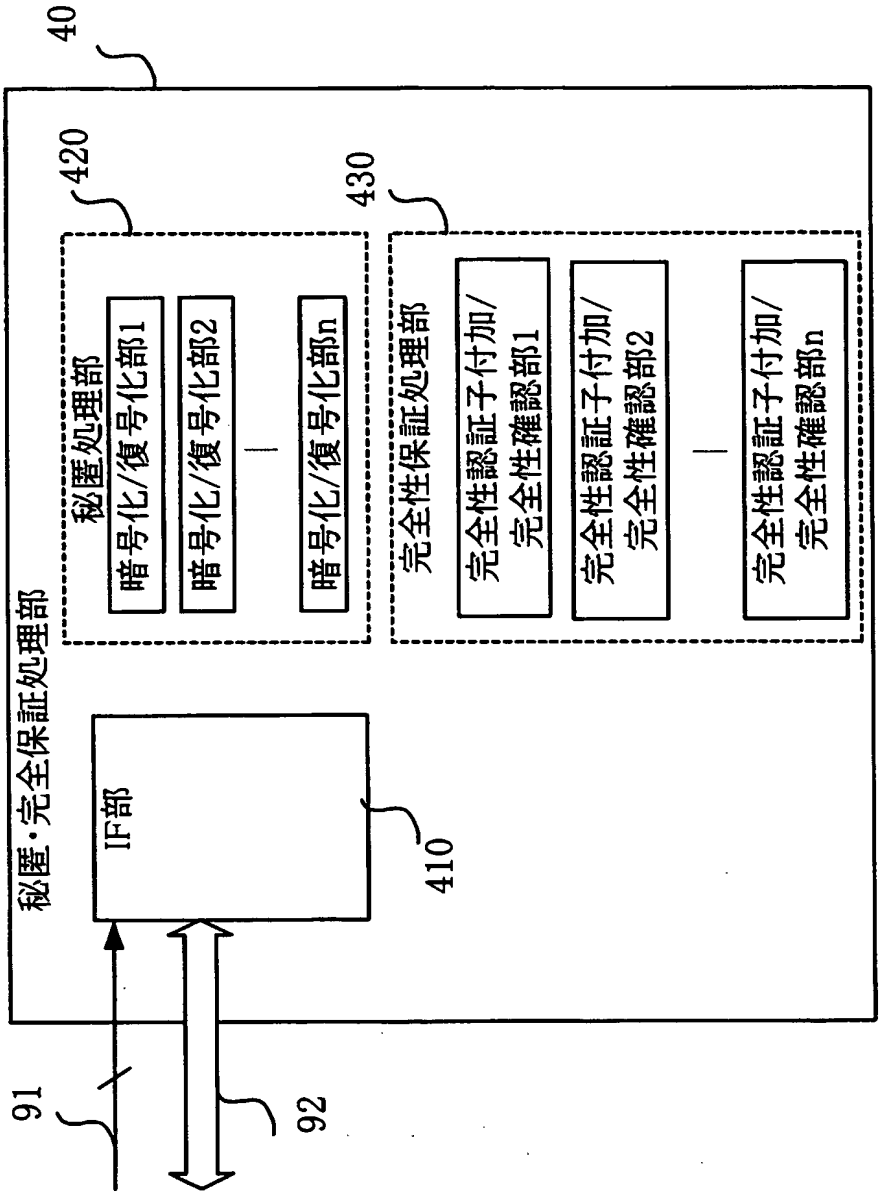

40
秘匿・完全保証処理部
420
秘匿処理部
暗号化/復号化部1
暗号化/復号化部2
暗号化/復号化部n
430
完全性保証処理部
完全性認証子付加/完全性確認部1
完全性認証子付加/完全性確認部2
完全性認証子付加/完全性確認部n
IF部
410
91
92

図 9

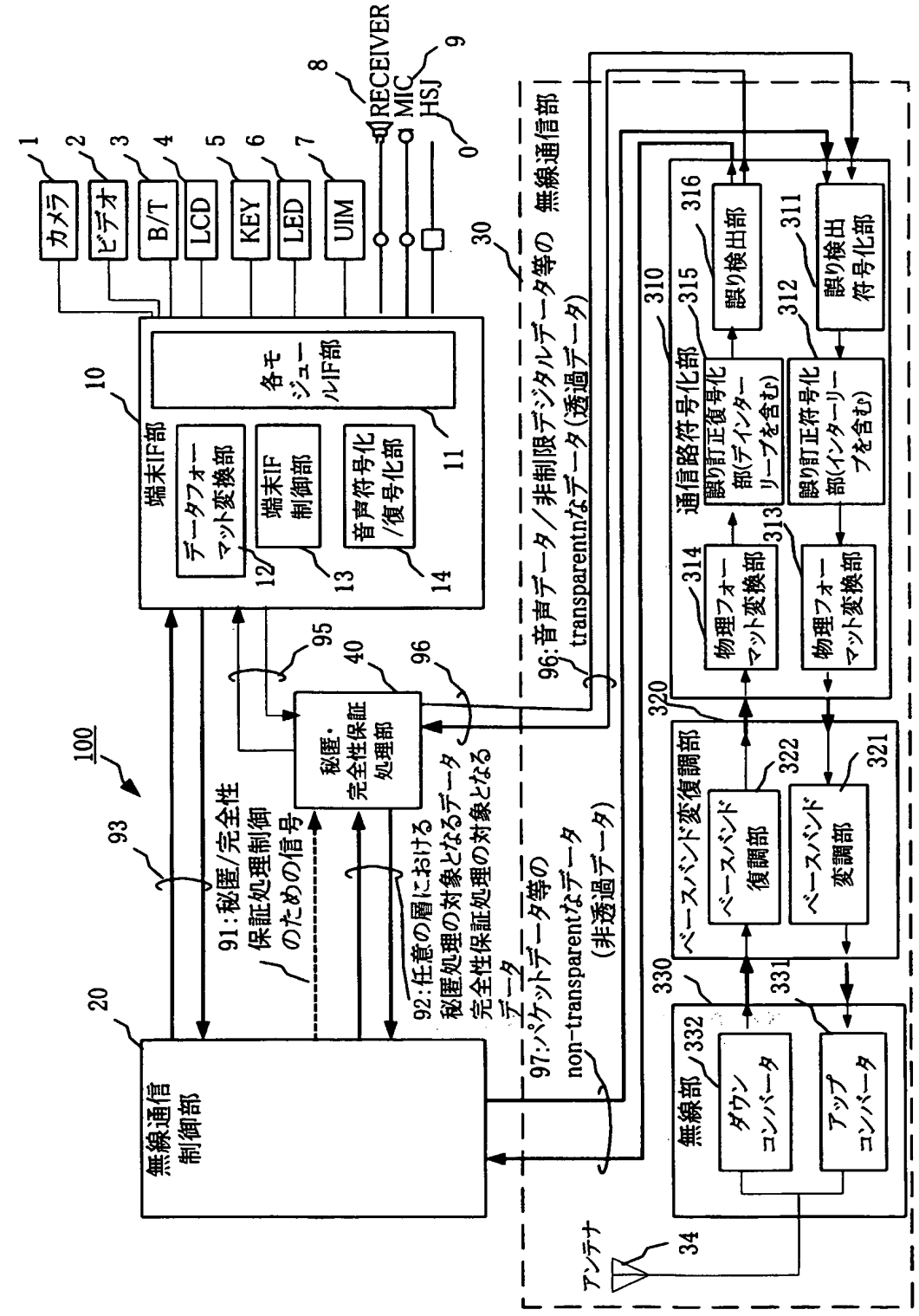

カメラ
ビデオ
B/T
LCD
KEY
LED
UIM
RECEIVER
MIC
HSJ
1
2
3
4
5
6
7
8
9
0
10
端末IF部
データフォーマット変換部
端末IF制御部
音声符号化/復号化部
各モジュールIF部
11
12
13
14
30
96;音声データ/非制限デジタルデータ等の transparentnなデータ(透過データ)
無線通信部
100
93
91:秘匿/完全性保証処理のための信号
秘匿・完全性保証処理部
40
95
96
92:任意の層における秘匿処理の対象となるデータ
完全性保証処理の対象となるデータ
97:パケットデータ等の non-transparentなデータ (非透過データ)
20
無線通信制御部
310
通信路符号化部
誤り訂正復号化部(デインターリーブを含む)
誤り検出部
315
316
誤り訂正符号化部(インターリーブを含む)
誤り検出符号化部
312
311
物理フォーマット変換部
物理フォーマット変換部
314
313
320
ベースバンド変復調部
ベースバンド復調部
ベースバンド変調部
322
321
330
無線部
ダウンコンバータ
アップコンバータ
332
331
アンテナ
34

図 10

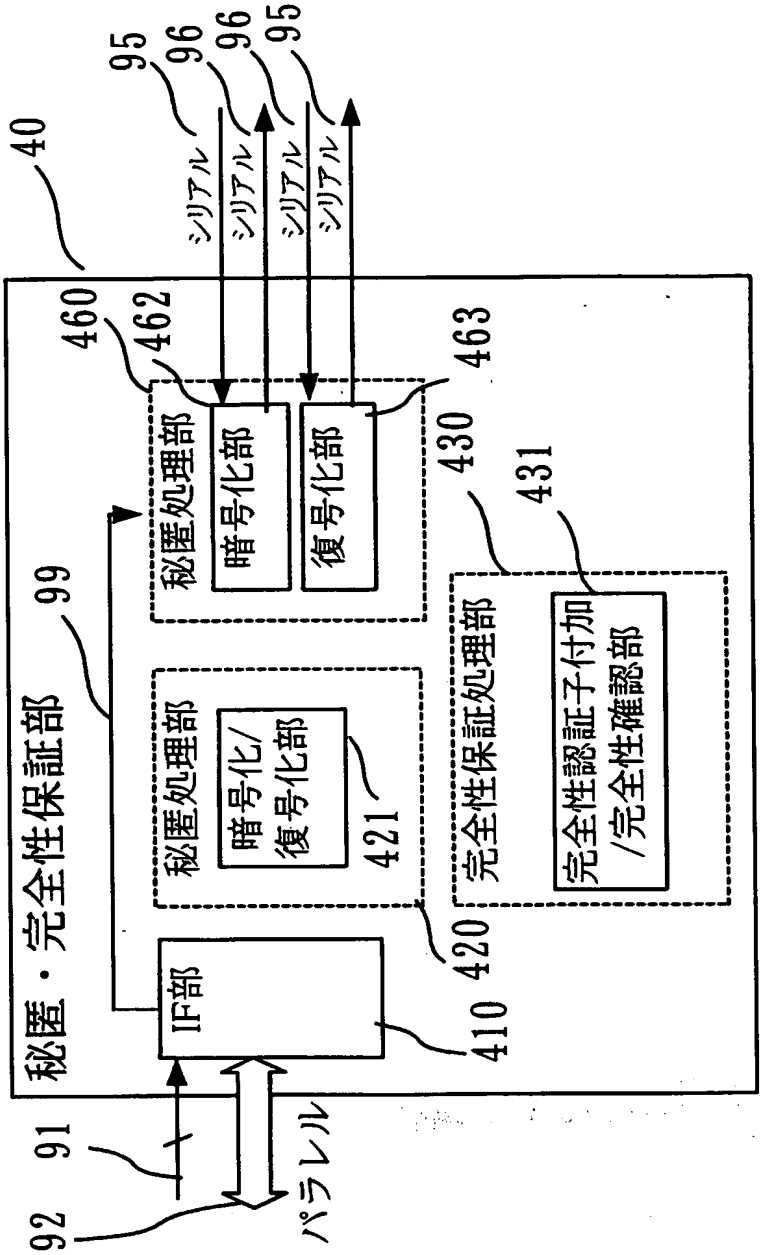

40
95
96
96
95
シリアル
シリアル
シリアル
シリアル
460
462
463
秘匿処理部
暗号化部
復号化部
430
431
秘匿処理部
暗号化/
復号化部
421
完全性保証処理部
完全性認証子付加
/完全性確認部
99
秘匿・完全性保証部
IF部
420
410
91
92
パラレル

図 11

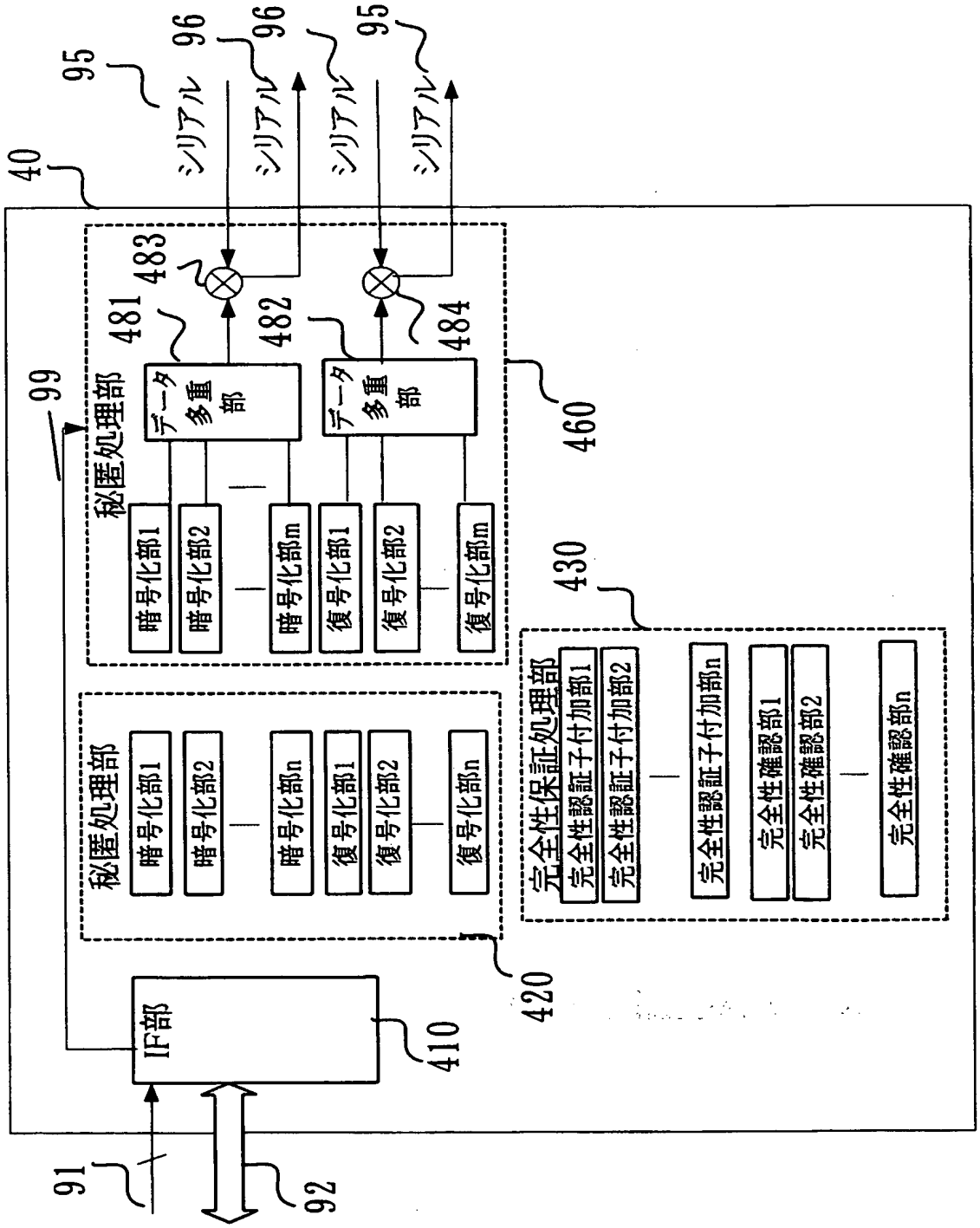

40
95
シリアル
96
シリアル
96
シリアル
95
シリアル
483
481
482
484
99
秘匿処理部
データ多重部
データ多重部
460
暗号化部1
暗号化部2
暗号化部m
復号化部1
復号化部2
復号化部m
430
完全性保証処理部
完全性認証子付加部1
完全性認証子付加部2
完全性認証子付加部n
完全性確認部1
完全性確認部2
完全性確認部n
秘匿処理部
暗号化部1
暗号化部2
暗号化部n
復号化部1
復号化部2
復号化部n
420
IF部
410
91
92

図 12

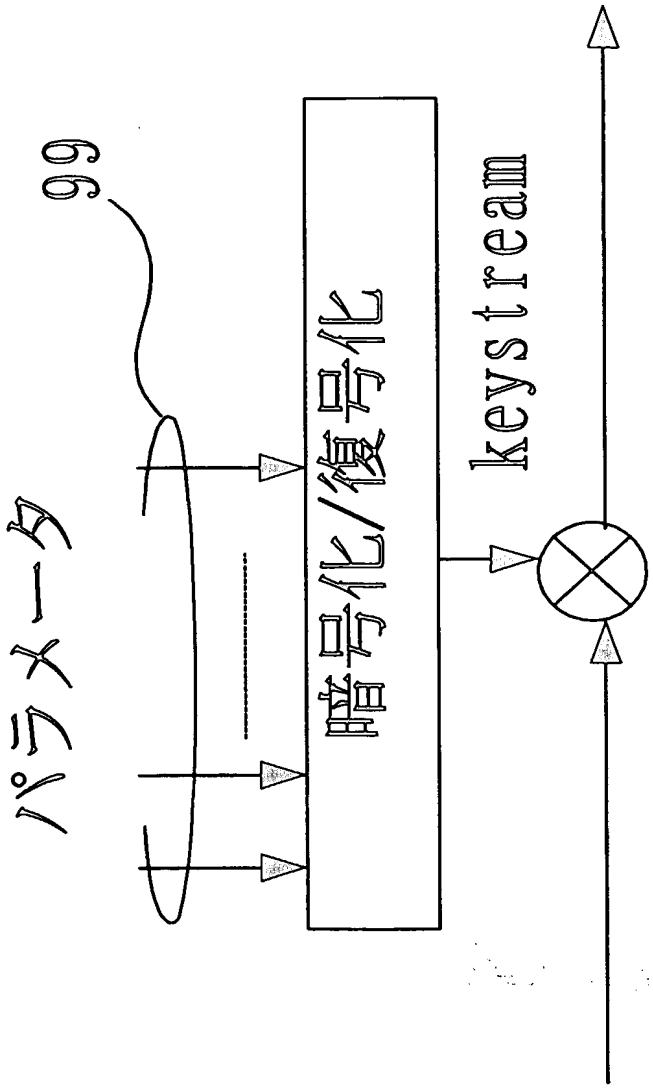


図 13

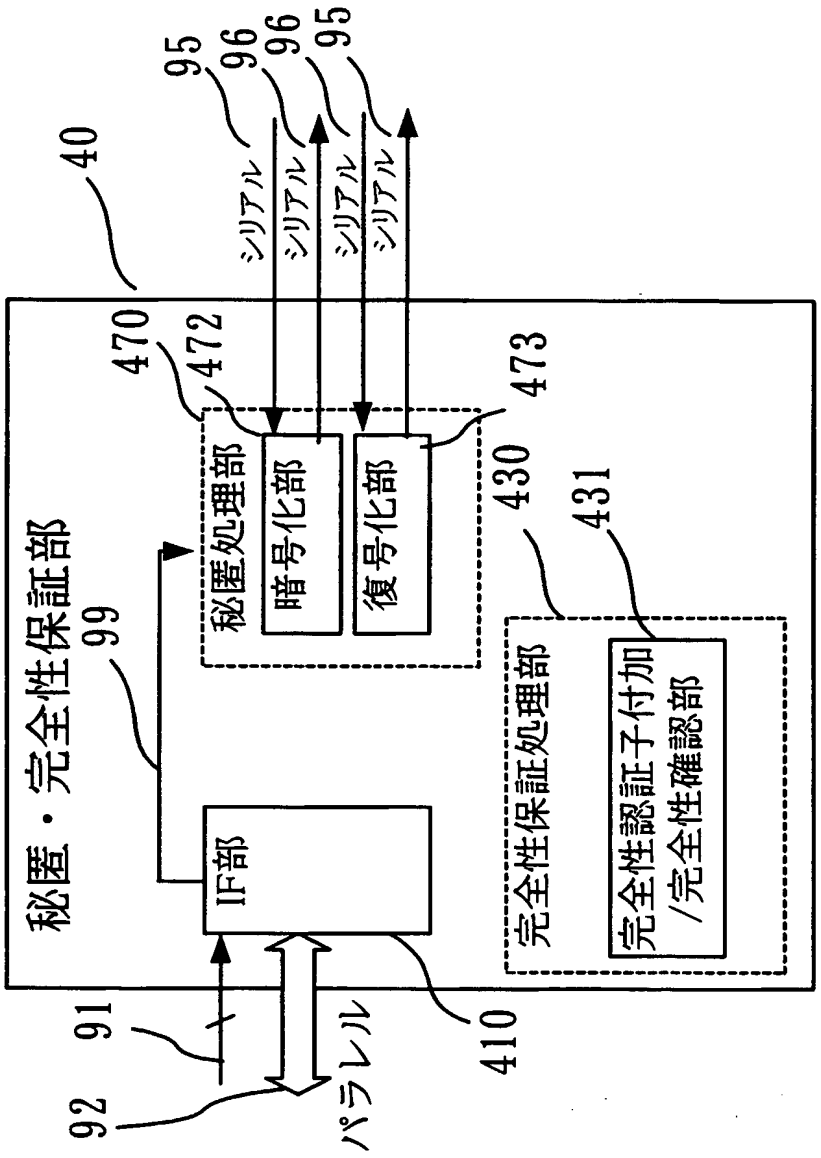

95
96
96
95
シリアル
シリアル
シリアル
シリアル
40
470
472
473
秘匿処理部
暗号化部
復号化部
430
431
完全性保証処理部
完全性認証子付加
/完全性確認部
秘匿・完全性保証部
99
IF部
91
92
パラレル
410

図14

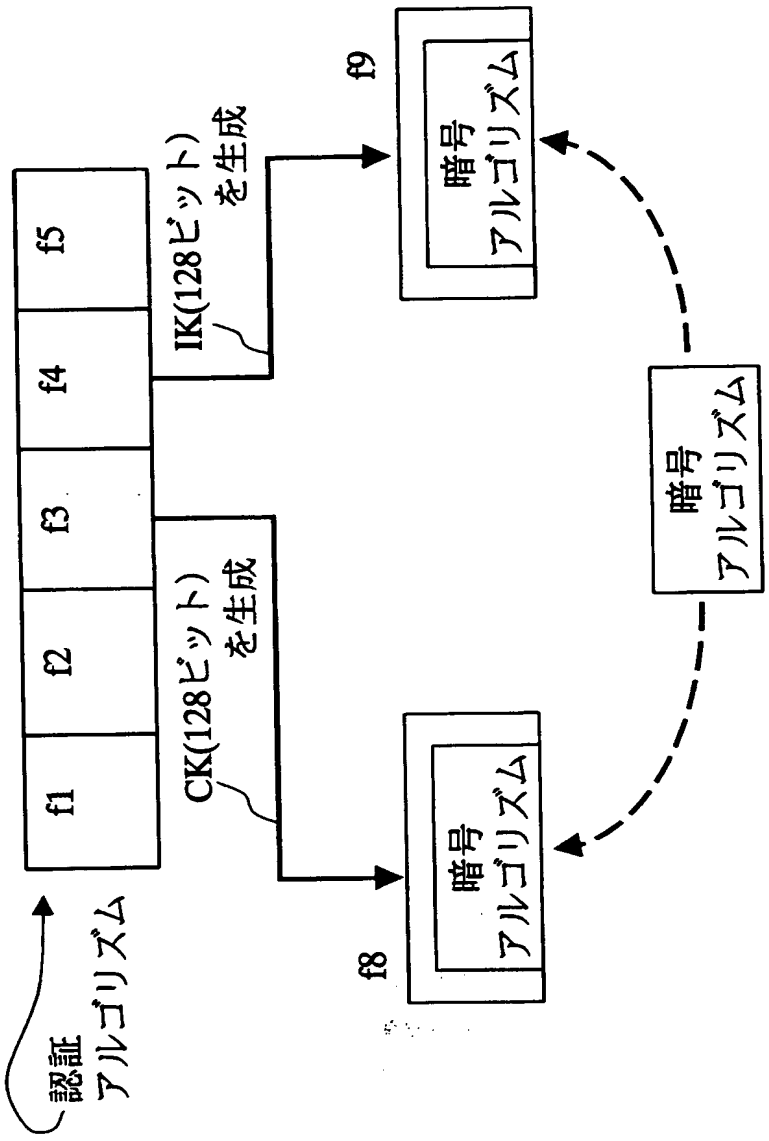

f1
f2
f3
f4
f5
認証
アルゴリズム
CK(128ビット)
を生成
IK(128ビット)
を生成
f8
暗号
アルゴリズム
暗号
アルゴリズム
f9
暗号
アルゴリズム

図 15

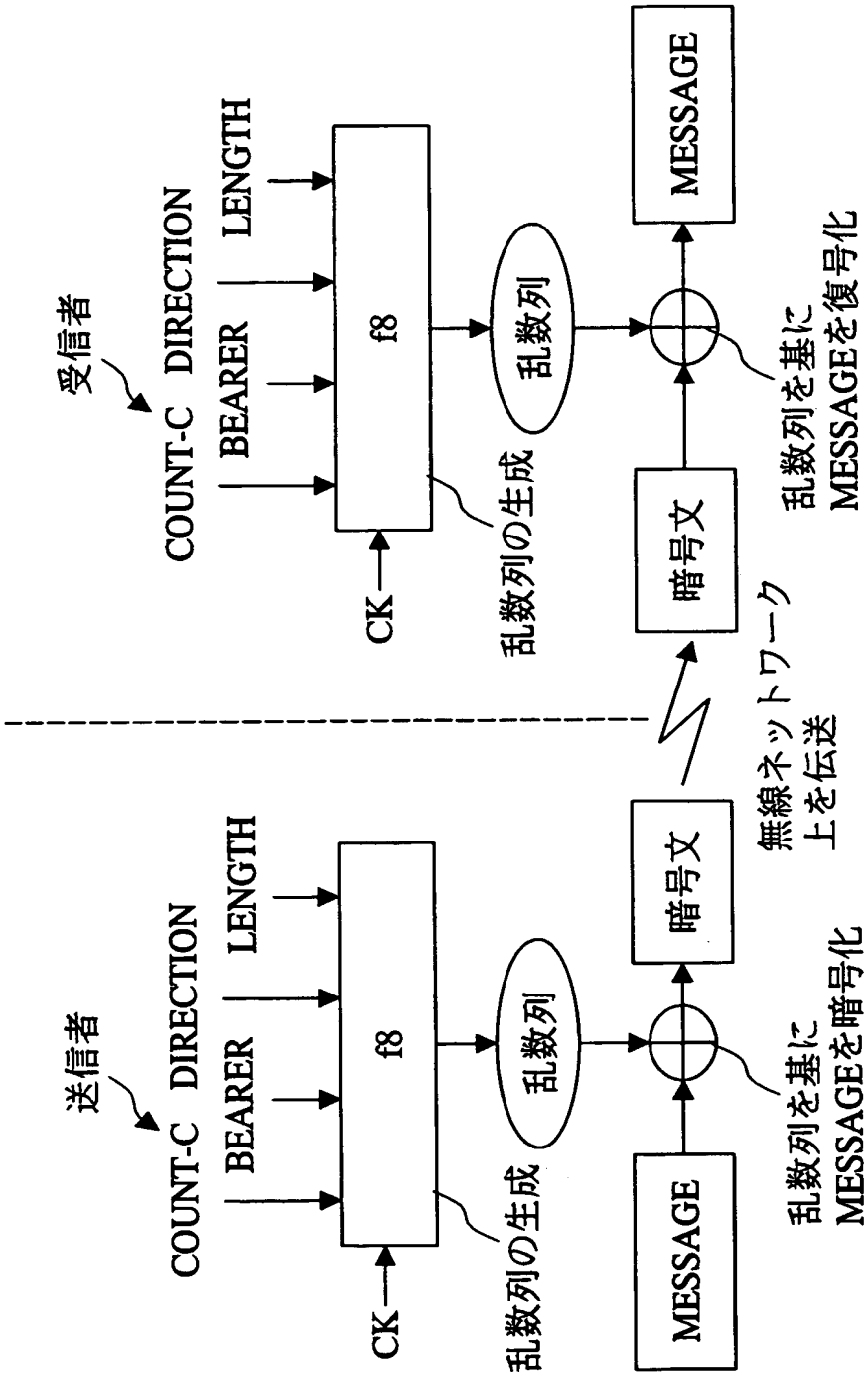

送信者
COUNT-C
DIRECTION
BEARER
LENGTH
f8
CK
乱数列の生成
乱数列
MESSAGE
暗号文
乱数列を基に
MESSAGEを暗号化
無線ネットワーク
上を伝送
受信者
COUNT-C
DIRECTION
BEARER
LENGTH
f8
CK
乱数列の生成
乱数列
暗号文
MESSAGE
乱数列を基に
MESSAGEを復号化

図 16

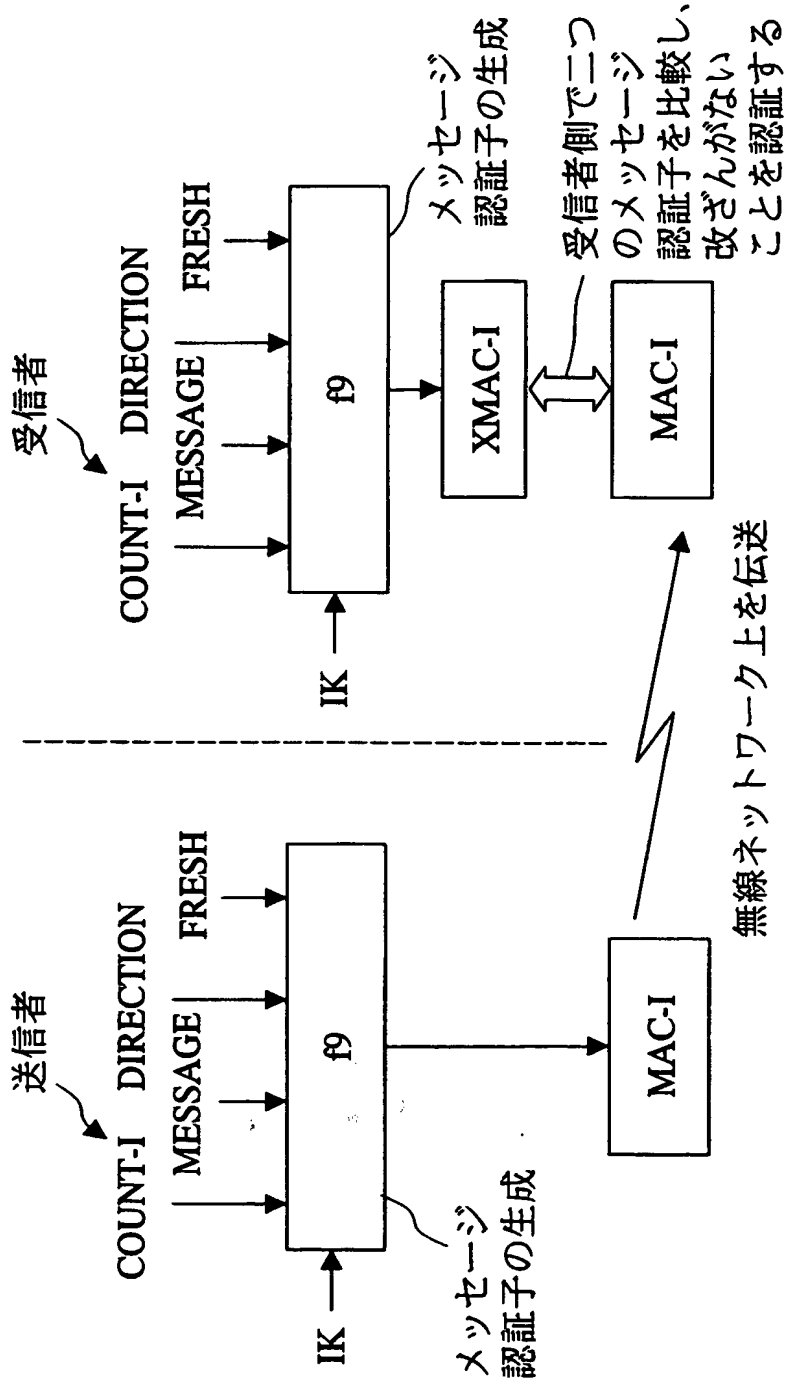

受信者
COUNT-I
DIRECTION
MESSAGE
FRESH
f9
IK
メッセージ
認証子の生成
XMAC-I
MAC-I
受信者側で二つ
のメッセージ
認証子を比較し、
改ざんがない
ことを認証する
送信者
COUNT-I
DIRECTION
MESSAGE
FRESH
f9
IK
メッセージ
認証子の生成
MAC-I
無線ネットワーク上を伝送

図17

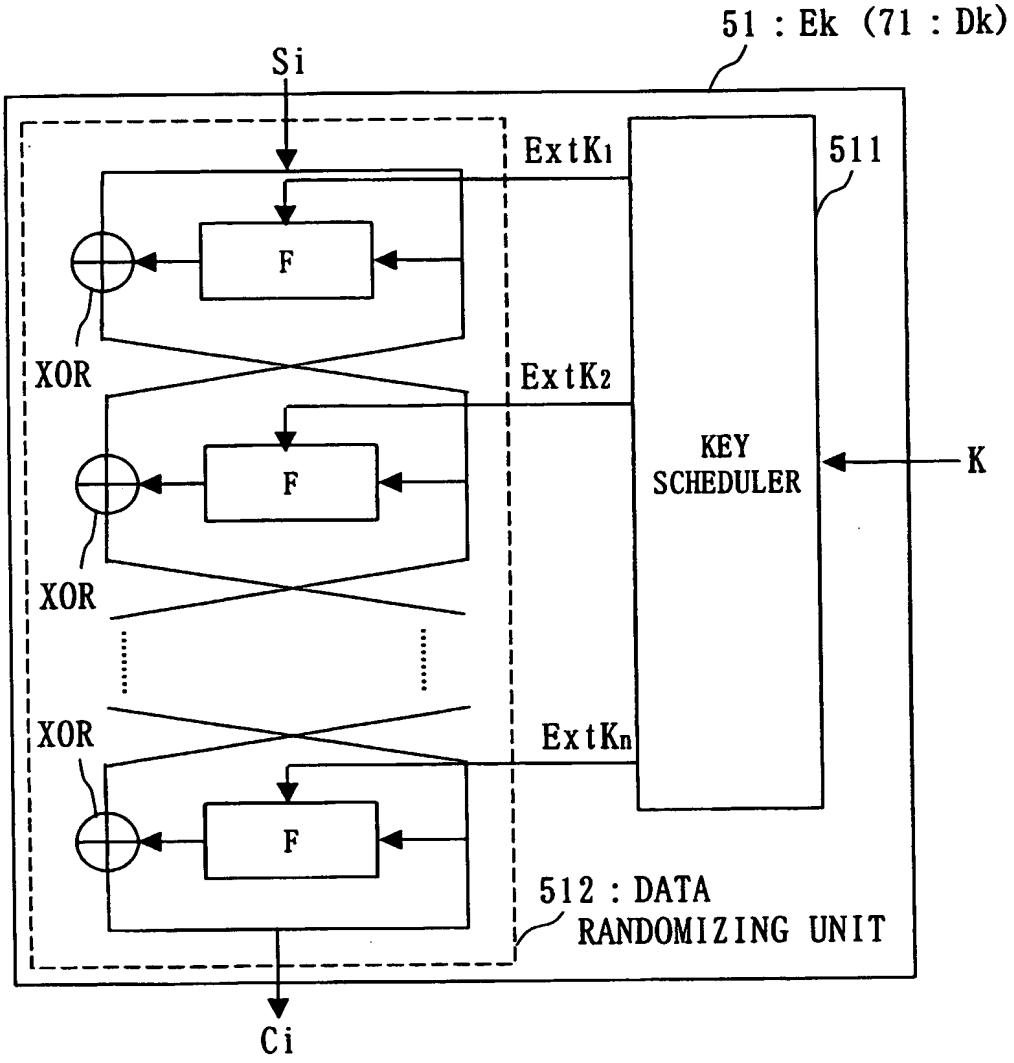

51 : Ek (71 : Dk)
Si
ExtK1
511
F
XOR
ExtK2
KEY
SCHEDULER
K
F
XOR
XOR
ExtKn
F
512 : DATA
RANDOMIZING UNIT
Ci

図18

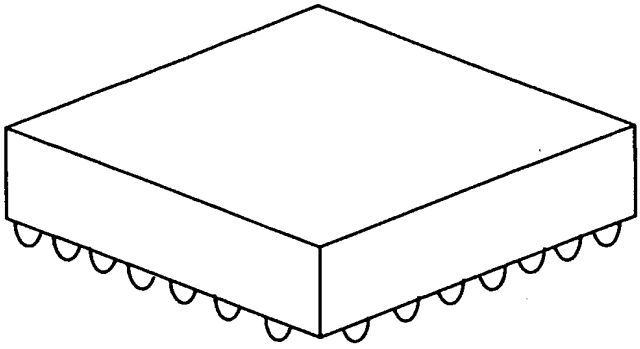


図19

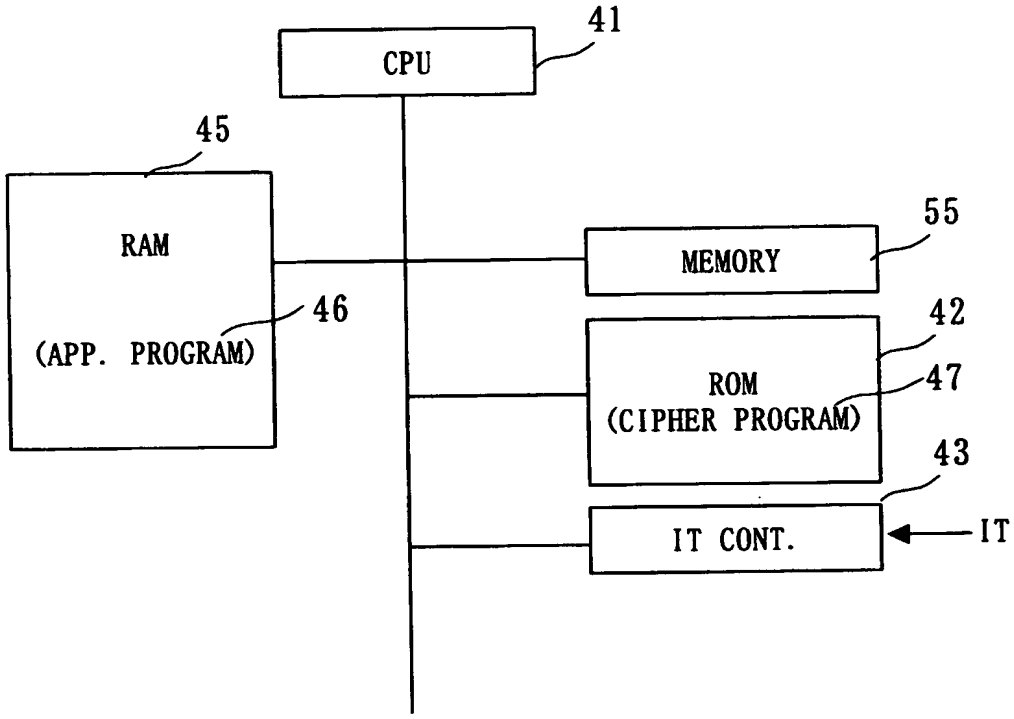

CPU
41
45
RAM
(APP. PROGRAM)
46
MEMORY
55
ROM
(CIPHER PROGRAM)
42
47
IT CONT.
43
IT

図20

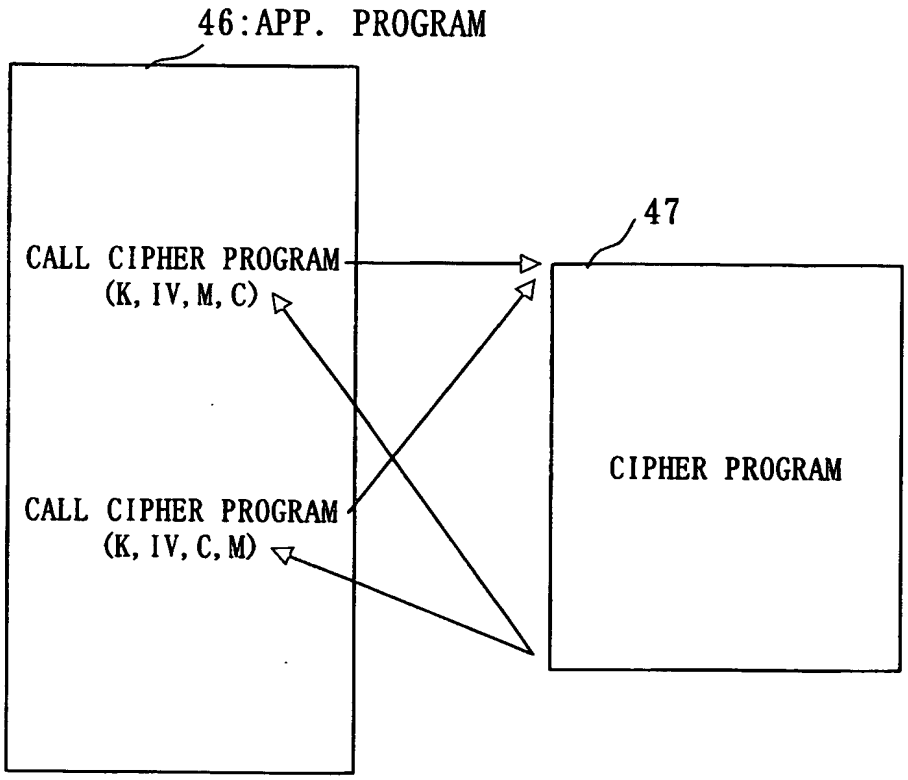

46:APP. PROGRAM
47
CALL CIPHER PROGRAM
(K, IV, M, C)
CALL CIPHER PROGRAM
(K, IV, C, M)
CIPHER PROGRAM

図21

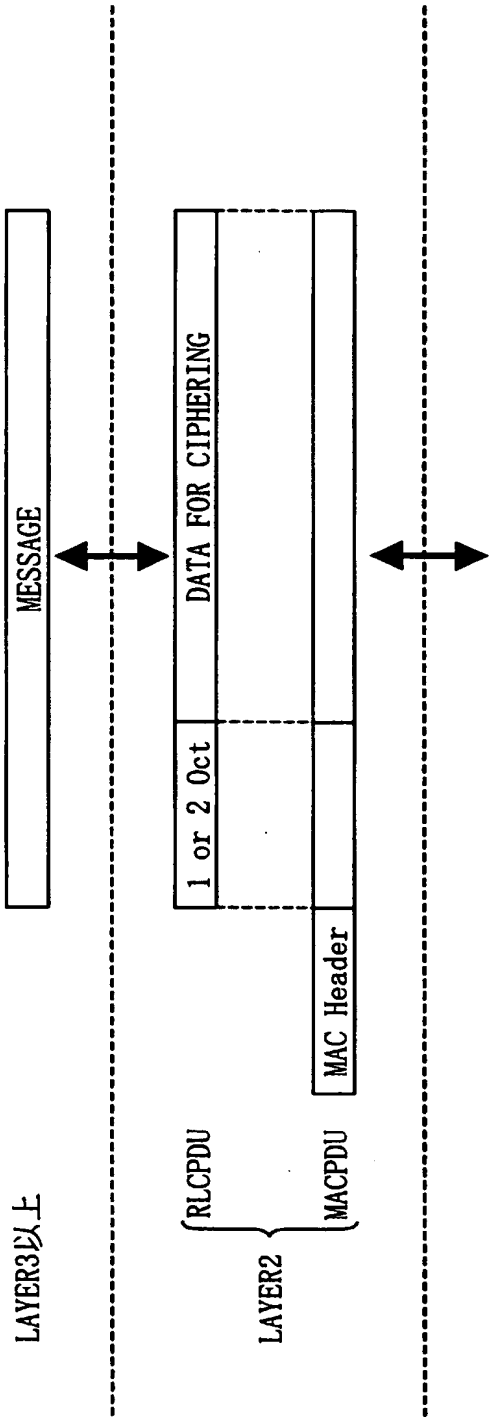

MESSAGE
DATA FOR CIPHERING
1 or 2 Oct
MAC Header
RLCPDU
MACPDU
LAYER3以上
LAYER2
LAYER1

図22

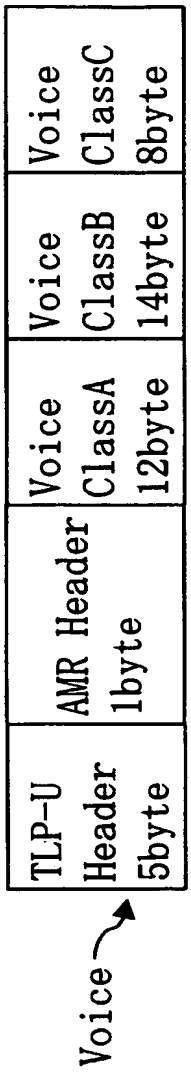

TLP-U Header 5byte
AMR Header 1byte
Voice ClassA 12byte
Voice ClassB 14byte
Voice ClassC 8byte
Voice

図23

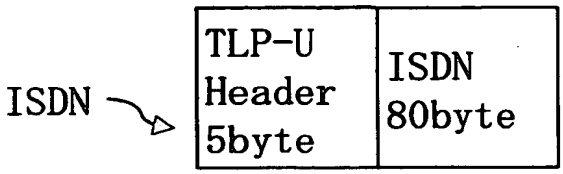
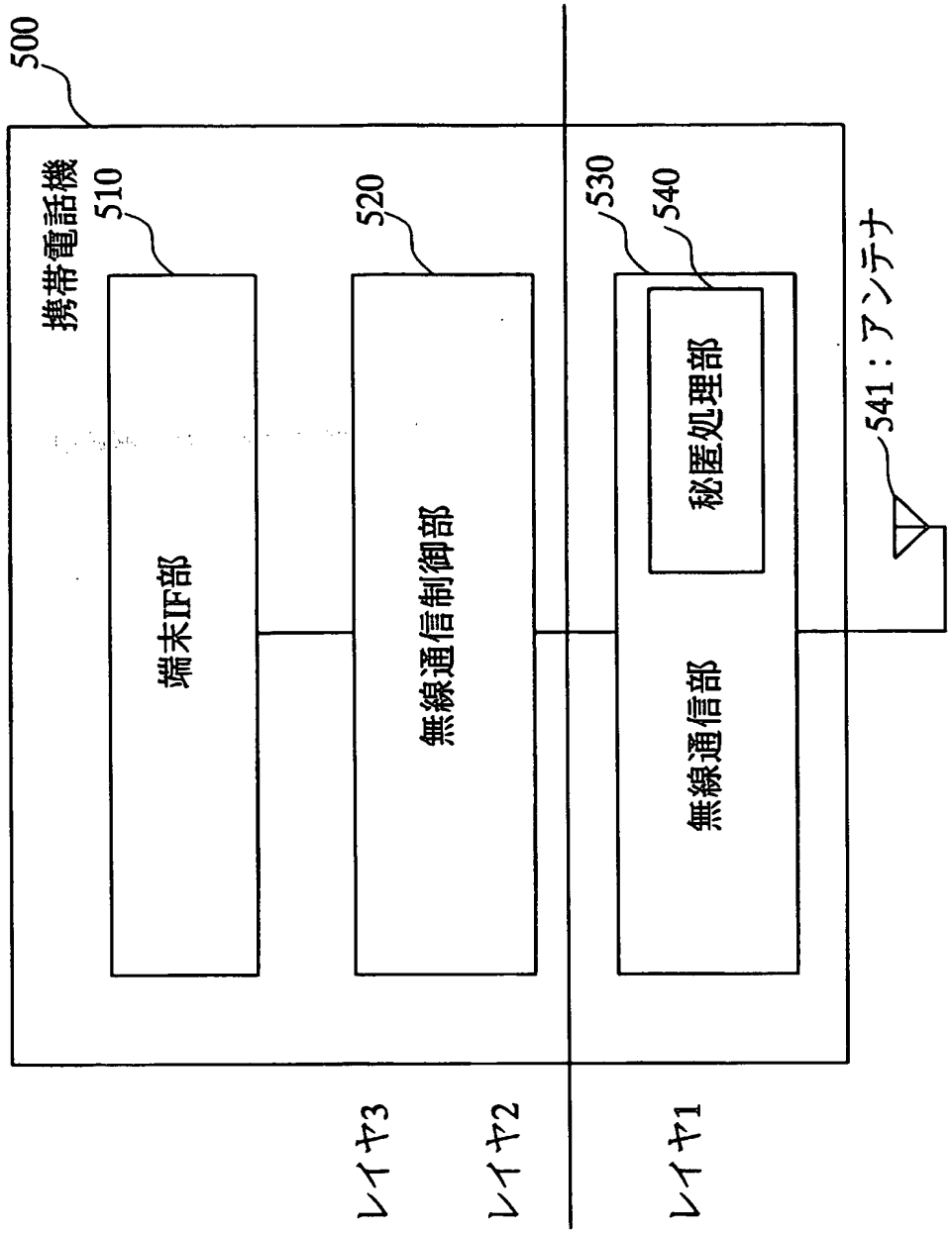


図 24


500
携帯電話機
510
端末IF部
520
無線通信制御部
530
無線通信部
540
秘匿処理部
541：アンテナ
レイヤ3
レイヤ2
レイヤ1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09128

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04Q 7/38, H04L 9/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04B 7/24-7/26, H04Q 7/00, G09C 1/00-5/00,
H04K 1/00-3/00, H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-22996, A (Mitsubishi Electric Corporation), 23 January, 1998 (23.01.98) & GB, 2314741, A & CA, 2205637, A & DE, 19721949, A1 & US, 6016350, A	1-38
Y	JP, 7-245606, A (NEC Corporation), 19 September, 1995 (19.09.95) (Family: none)	1-38
Y	JP, 7-327257, A (Hitachi, Ltd.), 12 December, 1995 (12.12.95) (Family: none)	1-38
Y	JP, 10-66157, A (Nokia Mobile Phones Ltd.), 06 March, 1998 (06.03.98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111,A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (Kokusai Electric Co., Ltd.), 29 January, 1993 (29.01.93) (Family: none)	1-38

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March, 2001 (12.03.01)	21 March, 2001 (21.03.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	D. W. Davies and W. L. Price; Translation supervised by Tadahiro Uezono "Network Security", Nikkei McGraw Hill (1985), pp. 77-78, pp.121-123	9,18,24-26

国際調査報告

国際出願番号　PCT／JP00／09128

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁷
H04Q 7／38　H04L 9／16

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁷
H04B 7／24－7／26　H04Q 7／00　G09C 1／00－5／00
H04K 1／00－3／00　H04L 9／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2001年
日本国登録実用新案公報　1994－2001年
日本国実用新案登録公報　1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP，10－22996，A（三菱電機株式会社） 23．1月．1998（23．01．98） & GB，2314741，A & CA，2205637，A & DE，19721949，A1 & US，6016350，A	1-38
Y	JP，7－245606，A（日本電気株式会社） 19．9月．1995（19．09．95）， （ファミリーなし）	1-38

☑ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
12．03．01	21.03.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	丸山　高政	5W	9570
	電話番号　03－3581－1101　内線　3574		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT/JP00/09128

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 7-327257, A (株式会社日立製作所) 12. 12月. 1995 (12. 12. 95), (ファミリーなし)	1-38
Y	JP, 10-66157, A (ノキア モービル フォーンズ リミティド) 6. 3月. 1998 (06. 03. 98) & GB, 2313989, A & FR, 2750272, A1 & FI, 9602352, A & SE, 9702172, A & US, 5987137, A & ES, 2143371, A1 & DE, 19723659, A1 & WO97/47111, A1 & AU, 9723703, A & AU, 9730346, A	1-38
A	JP, 5-22284, A (国際電気株式会社) 29. 1月. 1993 (29. 01. 93), (ファミリーなし)	1-38
Y	D. W. Davies and W. L. Price著, 上園忠弘監訳 「ネットワーク・セキュリティ」日経マグロウヒル, (昭和60年), pp. 77-78及び121-123	9, 18, 24-26